Programming Manual

Allen-Bradley

Logix5000 Controllers Security

Catalog Numbers 1756 ControlLogix, 1769 CompactLogix, 1789 SoftLogix, 1794 FlexLogix, PowerFlex 700S with DriveLogix

Allen-Bradley • Rockwell Software

Rockwell Automation

Important User Information

Solid-state equipment has operational characteristics differing from those of electromechanical equipment. Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (publication SGI-1.1 available from your local Rockwell Automation sales office or online at http://www.rockwellautomation.com/literature/) describes some important differences between solid-state equipment and hard-wired electromechanical devices. Because of this difference, and also because of the wide variety of uses for solid-state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

⚠	**WARNING:** Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
⚠	**ATTENTION:** Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence.
⚡	**SHOCK HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
♨	**BURN HAZARD:** Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.

Summary of Changes

This manual contains new and updated information.

IMPORTANT RSLogix 5000 programming software is now known as Studio 5000™ Logix Designer application, a component of the Studio 5000 Engineering and Design Environment.

The following controllers are no longer supported in the Logix Designer application, version 21.

Catalog Number	Description
1756-L61	ControlLogix 5561 Controller
1756-L61S	ControlLogix 5561S Controller
1756-L62	ControlLogix 5562 Controller
1756-L62S	ControlLogix 5562S Controller
1756-L63	ControlLogix 5563 Controller
1756-L63S	ControlLogix 5563S Controller
1756-L64	ControlLogix 5564 Controller
1756-L65	ControlLogix 5565 Controller
1768-L43	CompactLogix 5343 Controller
1768-L43S	CompactLogix 5343S Controller
1768-L45	CompactLogix 5345 Controller
1768-L45S	CompactLogix 5345S Controller
1769-L23E-QBF1	CompactLogix 5323E-QB1 Controller
1769-L23E-QBFC1	CompactLogix 5323E-QBFC1 Controller
1769-L23-QBFC1	CompactLogix 5323-QBFC1 Controller
1769-L31	CompactLogix 5331 Controller
1769-L32C	CompactLogix 5332C Controller
1769-L32E	CompactLogix 5332E Controller
1769-L35CR	CompactLogix 5335CR Controller
1769-L35E	CompactLogix 5335E Controller

Changes throughout this revision are marked by change bars, as shown in the margin of this page.

This table contains the changes made to this revision.

Topic	Page
Specifying a Source Key File	33
Securing a Logix Designer Application Project File	18, 19

Notes:

Preface

Chapter 1

Security

Chapter 2

Configuring FactoryTalk Security with Logix Designer Application

Chapter 3

Migrating from a Security Server Database to a FactoryTalk Server

Chapter 4

Configuring Source Protection in the Logix Designer Application

RSLogix 5000 Software CPU Security Tool

Chapter 5

Index

Studio 5000 Engineering and Design Environment and Logix Designer Application

The Studio 5000™ Engineering and Design Environment combines engineering and design elements into a common environment. The first element in the Studio 5000 environment is the Logix Designer application. The Logix Designer application is the rebranding of RSLogix™ 5000 software and will continue to be the product to program Logix5000™ controllers for discrete, process, batch, motion, safety, and drive-based solutions.

The Studio 5000 environment is the foundation for the future of Rockwell Automation® engineering design tools and capabilities. It is the one place for design engineers to develop all the elements of their control system.

Purpose of This Manual

This manual explains how to configure security for Logix Designer application. It also explains how to setup source protection for your logic and projects.

This manual is one of a set of related manuals that show common procedures for programming and operating Logix5000 controllers. For a complete list of common procedures manuals, see the *Logix5000 Controllers Common Procedures Programming Manual*, publication1756-PM001.

The term Logix5000 controller refers to any controller that is based on the Logix5000 operating system, such as the following:

- CompactLogix controllers
- ControlLogix controllers
- GuardLogix controller
- DriveLogix controllers
- SoftLogix5800 controllers

Additional Resources

These documents contain additional information concerning related products from Rockwell Automation.

Resource	Description
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, http://www.ab.com	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http://www.rockwellautomation.com/literature/. To order paper copies of technical documentation, contact your local Allen-Bradley distributor or Rockwell Automation sales representative.

Security

Introduction

This chapter discusses security related features available in the Logix Designer application.

In version 20 or later of the application, security enhancements provide:

- Security Server Validation - When enabled, and a user attempts to access a secured controller or project file, the application will make sure that the user is authorized by a FactoryTalk Directory trusted by that controller or project file. For more information, refer to "Securing a Logix Designer Application Project File" on page 16.
- Change Detection - Two new Controller attributes were added: ChangesToDetect and AuditValue. These attributes can be configured programmatically or by using the Security tab found in the Controller Properties dialog box. The audit value can be monitored from an HMI, historian, remote controller, and from Logix Designer application. For more information about Change Detection, see *Logix5000 Controllers Information and Status Programming Guide*, publication1756-PM015.
- Restricted communications through trusted slots - When enabled, ControlLogix controllers will only accept communications through selected slots. For more information about trusted slots, refer to "Securing a Logix Designer Application Project File" on page 16.

The Logix platform, version 18 or later, provides Data Access Control through two new tag attributes: External Access and Constant. Together, these attributes let you control access to tag data and help to safeguard tags by preventing unwanted changes to their values. For more information about Data Access Control, see the *Logix5000 Controllers I/O and Tag Data Programming Guide*, publication1756-PM004.

FactoryTalk Security

FactoryTalk Security integrates a common security model across all FactoryTalk enabled products. FactoryTalk Services Platform (FTSP) includes the FactoryTalk Administration Console that provides the interface for configuring your system.

FactoryTalk Directories

The FactoryTalk Directory is an important aspect to implementing FactoryTalk Security. In the FactoryTalk architecture, there are two separate Directory types, Local and Network. A FactoryTalk Local directory is sometimes utilized when all the Rockwell Automation Software products run on a single computer. The Local FactoryTalk Directory is used for products such as FactoryTalk View Machine Edition (ME) and FactoryTalk View Site Edition (SE) Station (Standalone). The FactoryTalk Network Directory is used when multiple Rockwell Automation Software products need to share information across multiple computer systems. The FactoryTalk Network Directory allows these systems to share a common FactoryTalk Directory for products, such as FactoryTalk View SE, FactoryTalk Integrator, FactoryTalk Batch, and FactoryTalk AssetCenter.

IMPORTANT In version 20 or later of the application, the FactoryTalk Local Directory is not supported.

When securing controllers using version 20 or later of the application, only the Network Directory is supported. If you are securing controllers using an earlier version of the application, you can use either the FactoryTalk Local Directory or the Network Directory. If you are trying to coordinate security across multiple computers, you will need a Network Directory implementation of FactoryTalk Security. If all of your products reside on a single computer, you can utilize the Local Directory. If you have a choice, you might want to use the Network Directory for forward compatibility with version 20 and later. The Network Directory can be locally hosted on each machine just like the Local Directory.

For more information about FactoryTalk Security, see the *FactoryTalk Security System Configuration Guide*, publication FTSEC-QS001.

Configuring FactoryTalk Security with Logix Designer Application

Introduction

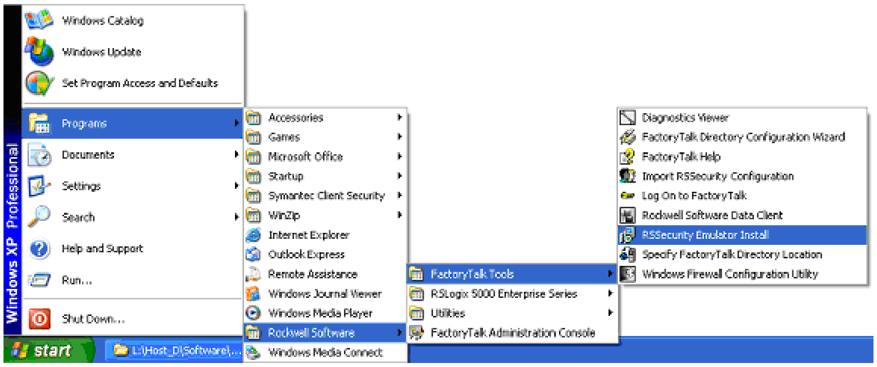
FactoryTalk Services Platform (FTSP) software is installed during the installation of the Logix Designer application.

Installing the Rockwell Software Security Emulator

RSLogix 5000 software version 19 or earlier, uses the Rockwell Software Security Emulator to communicate with FactoryTalk Security. Starting with version 20, RSLogix 5000 obtains security information directly from FactoryTalk Services Platform and does not require RSSecurity Emulator.

If you are using RSLogix 5000 version 19 or earlier, follow these instructions to install the Rockwell Software Security Emulator.

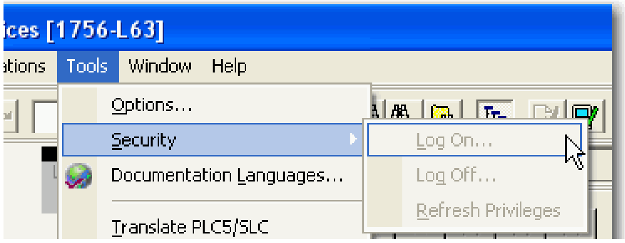
1. From the Start menu select **Programs>Rockwell Software>FactoryTalk Tools>RSSecurity Emulator Install**



2. Follow the installation prompts to complete the installation.

Enabling Security

If the Security menu is dimmed, as shown in this picture, you need to enable security for the application.

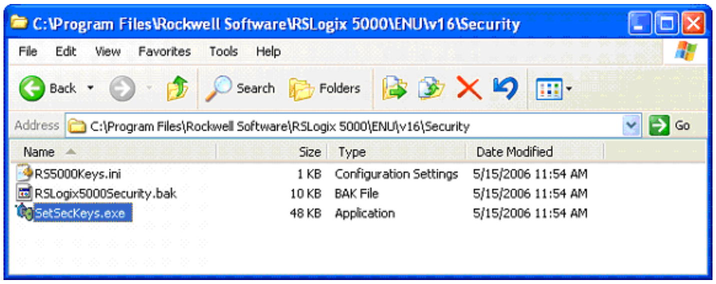


For version 20 or later of the application, if the security menu is dimmed, you need to install FactoryTalk Services Platform. See "Installing FactoryTalk Services Platform Software" on 15. If you are using version 20 or later, and the security menu is enabled, skip to step 5.

If you are using RSLogix 5000 version 19 or earlier, you need to use SetSecKeys to enable security. Follow the instructions below.

1. For RSLogix 5000 v19 or earlier, the SetSecKeys software is added to the system during installation.

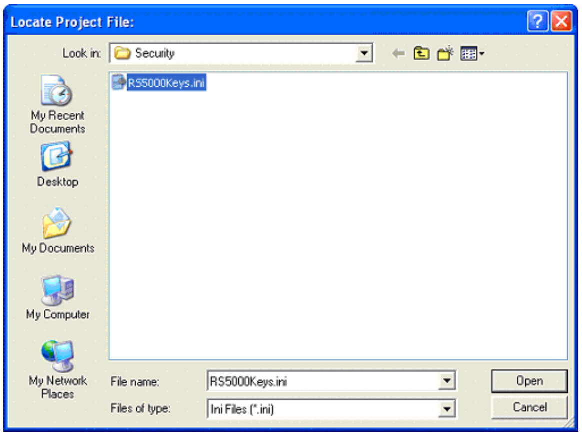
   Navigate to: **Program Files\Rockwell Software\RSLogix 5000\ENU\*vxx*\Security and double-click SetSecKeys.exe**. For this example, we are using RSLogix 5000 v16.


C:\Program Files\Rockwell Software\RSLogix 5000\ENU\v16\Security
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
Go

Address: C:\Program Files\Rockwell Software\RSLogix 5000\ENU\v16\Security

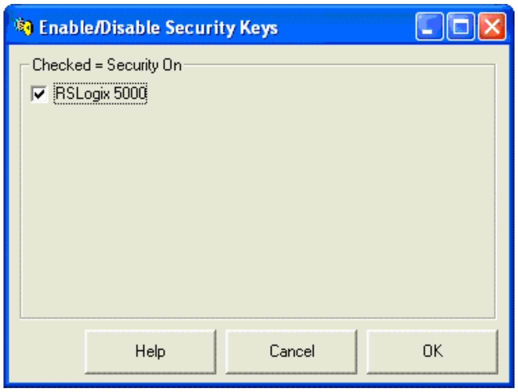
Name	Size	Type	Date Modified
RS5000Keys.ini	1 KB	Configuration Settings	5/15/2006 11:54 AM
RSLogix5000Security.bak	10 KB	BAK File	5/15/2006 11:54 AM
SetSecKeys.exe	48 KB	Application	5/15/2006 11:54 AM

2. If prompted to locate the project file, select the **RS5000Keys.ini** file and click **Open**.



ATTENTION: For RSLogix 5000 version 19 or earlier, if you need to disable FactoryTalk Security for RSLogix 5000, please contact Rockwell Automation Technical Support.

3. In the Enable/Disable Security Keys dialog box, select the **RSLogix 5000** check box and then click **OK**.



4. If the RSLogix 5000 Security: Enable dialog box appears, click **OK**.

5. Open the FactoryTalk Administration Console:
   a. Click **Start > All Programs > Rockwell Software > FactoryTalk Administration Console**.
   b. Select the **FactoryTalk Directory** option and click **OK**.

IMPORTANT	For version 20 or later of the application, security settings are obtained from the FactoryTalk Network Directory. RSSecurity Emulator is not required and the FactoryTalk Local Directory is not supported.

   c. If prompted to log on to FactoryTalk, enter your FactoryTalk user name and password, and then click **OK**.

TIP	If you cannot log on to FactoryTalk, see "I cannot log on to the FactoryTalk Directory" in FactoryTalk Help.

6. Open the RSLogix 5000 Feature Security Properties dialog box:
   a. In the Explorer window, navigate to:
   System > Policies > Product Policies > RSLogix 5000.
   b. Right-click **Feature Security** and select **Properties**.

7. Secure the RSLogix 5000 controller:
   a. In the Feature Security Properties dialog box, select **Controller:Secure** and then click **Browse**.
   b. In the Configure Securable Action dialog box, click **Add** to select the user accounts or groups that you want to configure.
   c. In the Select User and Computer dialog box, select the user accounts or groups and click **OK**.
   d. Follow the instructions to complete the configuration.

Installing FactoryTalk Services Platform Software

If you find that the Security feature is not enabled in the Logix Designer application you will need to make sure FactoryTalk Services Platform (FTSP) software is installed properly.

Follow these instructions to install the FTSP software.

1. On the installation disk, browse to **D:\System\FTSP** and double-click the **Setup.exe** file.
2. Follow the installation prompts to complete the installation.

   During the installation, all existing local and network FactoryTalk Directory files are automatically configured and backed up. For new installations, the pre-configured FactoryTalk Directory files are backed up. The backups let you restore the Factory Talk Directory files to a previous software version.

After the installation is complete, refer back to "Enabling Security" on page 12

If you are having problems, refer to the *FactoryTalk Security System Configuration Guide*, publication FTSEC-QS001.

Securing a Logix Designer Application Project File

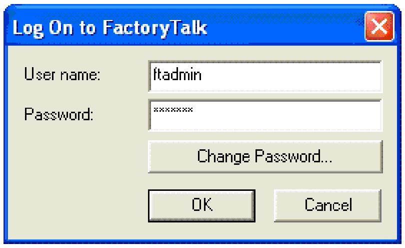
Once you have configured the Logix Designer application to be security aware, the next step is to enable security in a project file. Follow these steps to secure a project file.

1. Open Logix Designer.

   a. Click **Start > Rockwell Software>Studio 5000**.

   b. If prompted to Log On to FactoryTalk, enter your FactoryTalk user name and password, and then click **OK**.

   In the example below, the FactoryTalk Directory (FTD) was configured with an account called FTADMIN.



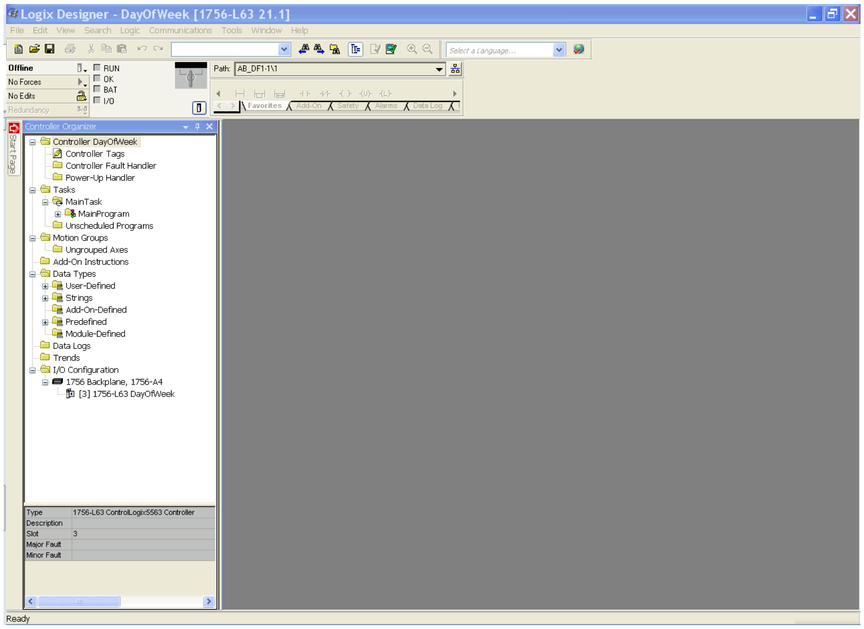
Log On to FactoryTalk

User name: ftadmin

Password: *******

2. Open the project file that you want to secure.

   This example uses the DayOf Week project file, which is provided on the installation CD.

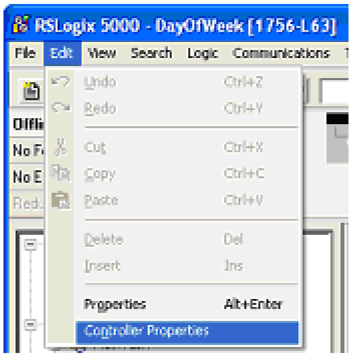


Logix Designer - DayOfWeek [1756-L63 21.1]

Path: AB_DF1-1\1

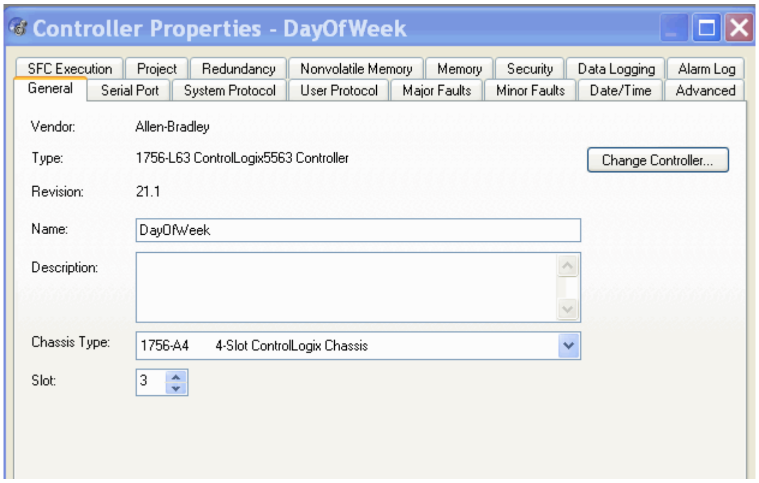
Type	1756-L63 ControlLogix5563 Controller
Description	
Slot	3
Major Fault	
Minor Fault	

3. On the Edit menu, click **Controller Properties**.



4. Click the **General** tab to find the controller name. Write down the name that appears in the Name field. By default, this is the name of the ACD file that will be used later on page 21when setting security in the FactoryTalk Administration Console.

   In this example, the name is DayOf Week.



Vendor: Allen-Bradley

Type: 1756-L63 ControlLogix5563 Controller

Revision: 21.1

Name: DayOfWeek

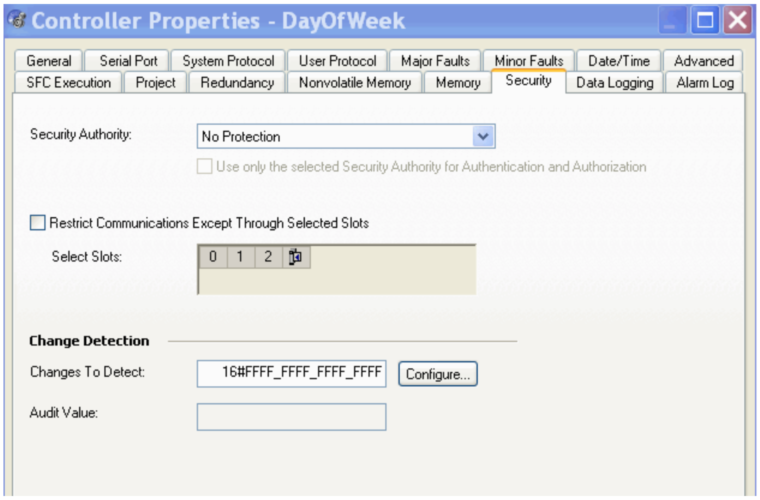
Description:

Chassis Type: 1756-A4 4-Slot ControlLogix Chassis

Slot: 3

5. To configure the security settings, click the **Security** tab or the **Advanced** tab depending on the version of the application.

   - Click the **Security** tab if it appears in the Controller Properties dialog box.



Security Authority: No Protection

□ Use only the selected Security Authority for Authentication and Authorization

□ Restrict Communications Except Through Selected Slots

Select Slots: 0 1 2 3

Change Detection

Changes To Detect: 16#FFFF_FFFF_FFFF_FFFF

Audit Value:

a. In the Security Authority list, select **FactoryTalk Security**.

IMPORTANT	When you select a security authority for a project, you can only access the project and any controller that contains it when you have been granted access in Factory Talk Security.

b. To associate the project with a specific authority, select the **Use only the selected Security Authority for Authentication and Authorization** check box.
To remove the association to the specified Security Authority for this project, go online with the controller and then clear this check box.

When you associate a project with a specific Security Authority, you are associating the project with a specific FactoryTalk Network Directory that is identified by a security authority identifier. Projects that are secured and bound to a specific Security Authority cannot be recovered if the security authority identifier of the FactoryTalk Network Directory used to secure the project no longer exists.

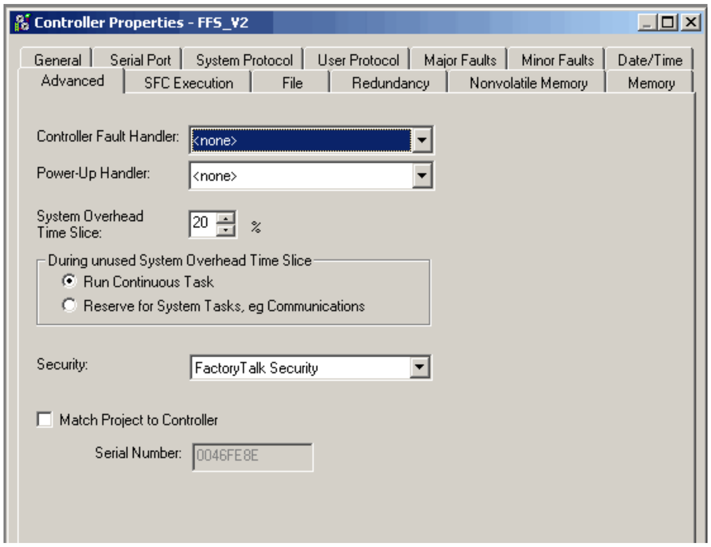
IMPORTANT	Before you associate this project with a specific Security Authority, we recommend that you back up the FactoryTalk Directory and save unsecured versions of this project file in (.ACD) or (.L5X or .L5K) formats, and save them in a secure location. For details about backing up a FactoryTalk Directory see the FactoryTalk Help: **Start > Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help**.

TIP	The check box is available when you are using FactoryTalk Services Platform 2.50 or later and a version of the application that supports associating a project with a specific Security Authority.

c. For information about the settings found on the Security tab such as, Restrict Communications Except Through Selected Slots, Selected Slots, or Change Detection, access the help from the Help menu.

- Click the **Advanced** tab, if the Security tab does not appear in the Controller Properties dialog box.

a. In the Security list select **FactoryTalk Security**.



Controller Properties - FFS_V2

Controller Fault Handler: <none>

Power-Up Handler: <none>

System Overhead Time Slice: 20 %

During unused System Overhead Time Slice

● Run Continuous Task

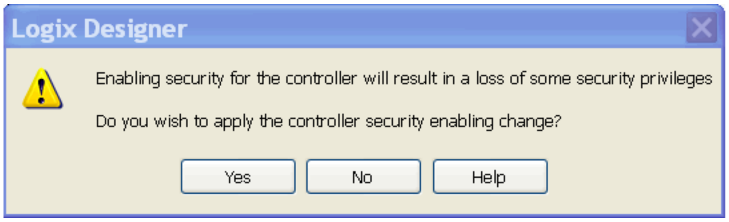
○ Reserve for System Tasks, eg Communications

Security: FactoryTalk Security

□ Match Project to Controller

Serial Number: 0046FE8E

6. Click **OK**. If prompted to confirm whether to confirm the controller settings, click **Yes**.



Logix Designer

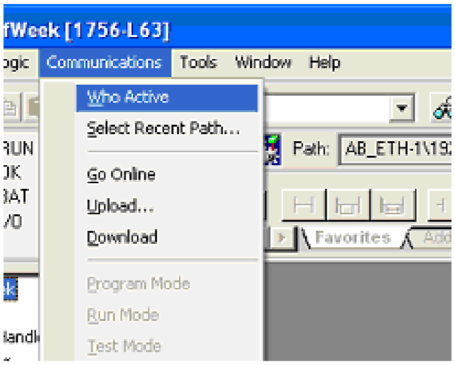
Enabling security for the controller will result in a loss of some security privileges

Do you wish to apply the controller security enabling change?

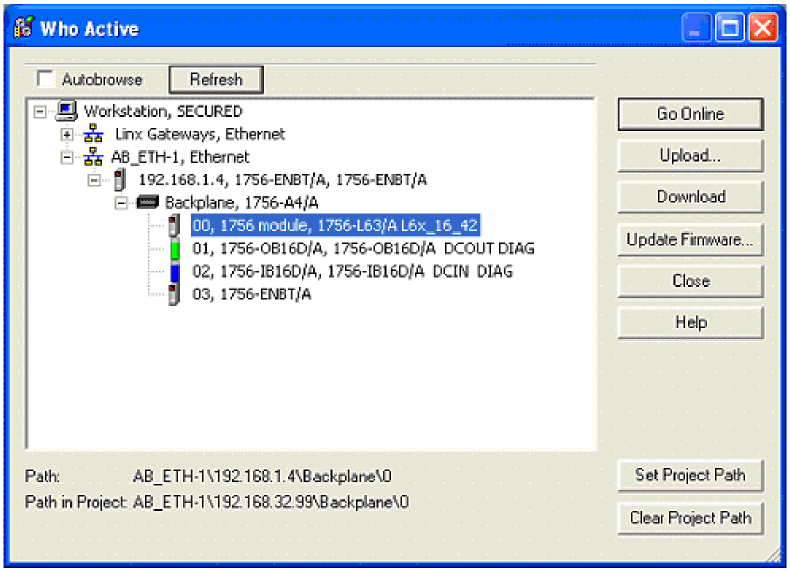
IMPORTANT When you select a security authority for a project, you can only access the project and any controller that contains it when you have been granted access in Factory Talk Security.

7. Save the project file.

8. To download the project file to the controller, on the Communications menu, click **Who Active**.



9. In the Who Active window, locate and select the controller resource.

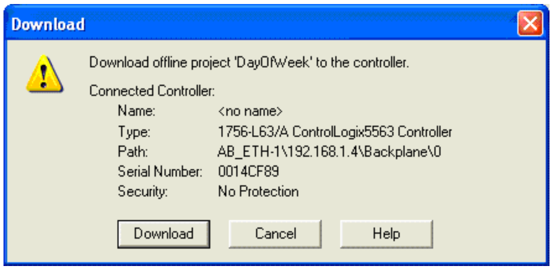


```
Workstation, SECURED
  Linx Gateways, Ethernet
  AB_ETH-1, Ethernet
    192.168.1.4, 1756-ENBT/A, 1756-ENBT/A
      Backplane, 1756-A4/A
        00, 1756 module, 1756-L63/A L6x_16_42
        01, 1756-OB16D/A, 1756-OB16D/A DCOUT DIAG
        02, 1756-IB16D/A, 1756-IB16D/A DCIN DIAG
        03, 1756-ENBT/A
```

Path: AB_ETH-1\192.168.1.4\Backplane\0

Path in Project: AB_ETH-1\192.168.32.99\Backplane\0

10. Click **Download** to continue.



Download offline project 'DayOfWeek' to the controller.

Connected Controller:

Name:	<no name>
Type:	1756-L63/A ControlLogix5563 Controller
Path:	AB_ETH-1\192.168.1.4\Backplane\0
Serial Number:	0014CF89
Security:	No Protection

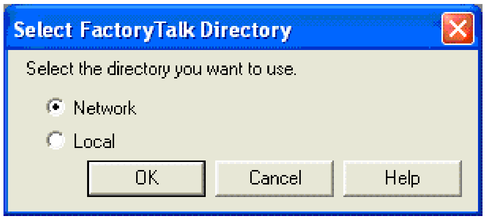
11. When the download is complete, close the application. If prompted, save changes.

Applying Security to a Controller Resource

In the following steps, a single controller is configured for security. When managing large numbers of users and controllers, Rockwell Automation recommends that you group users with user groups, group permissions with action groups, and use the Resource Grouping method to secure your resources to simplify administration of permissions. For details see the FactoryTalk Help: **Start** > **Programs** > **Rockwell Software** > **FactoryTalk Tools** > **FactoryTalk Help**.

Follow these steps to apply security to a controller resource.

1. Open the FactoryTalk Administration Console, select **Start>Programs >Rockwell Software>FactoryTalk Administration Console**.
2. Select the FactoryTalk Directory option and click **OK**.



Select FactoryTalk Directory

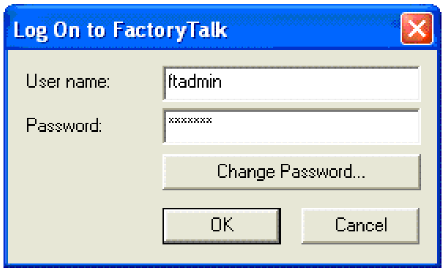
Select the directory you want to use.

● Network
○ Local

– For version 20 or later of the application, security settings are obtained from the FactoryTalk Network Directory. RSSecurity Emulator is not required and the FactoryTalk Local Directory is not supported.

– The default FactoryTalk Security configuration has Single Sign On enabled, so the you will not be prompted to Log On to FactoryTalk. Customers upgrading from revisions prior to 16.03 or customers that have modified the default FactoryTalk Security configuration will be prompted to Log On to FactoryTalk.

3. If prompted to Log On to FactoryTalk, enter your user name and password.
   In the example below, the FactoryTalk Directory (FTD) was configured with an account called FTADMIN.

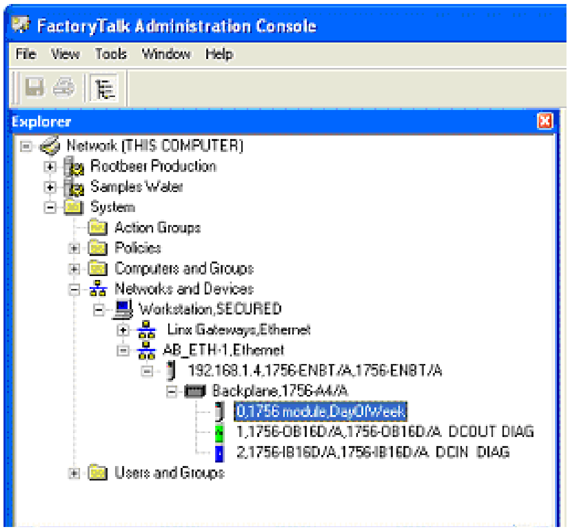


Log On to FactoryTalk

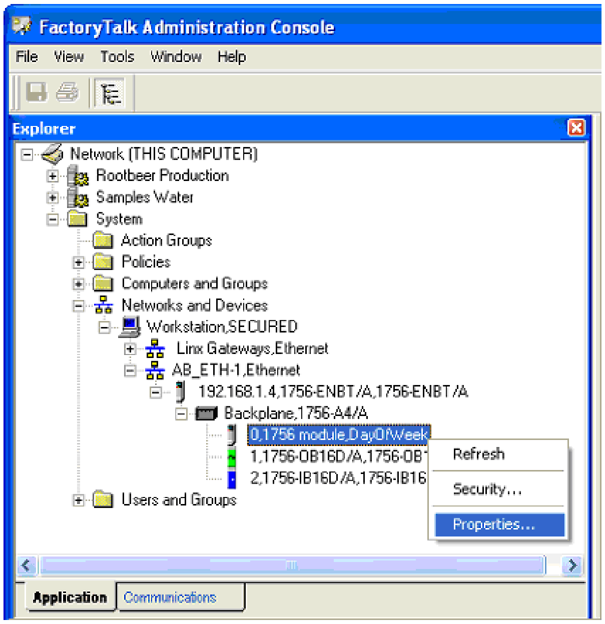
User name: ftadmin

Password: *******

4. Navigate to the controller resource the secured project file was downloaded to.
   From the Explorer window, expand Networks and Devices and navigate to the controller you want to configure.



5. Right-click on the controller resource and select **Properties**.



EXAMPLE If you want the security settings to be inherited by all controllers, right click on **Networks and Devices**, then select **Security**. From the Security Settings dialog, you can configure security settings that will be inherited by all secured projects. Unique permissions can still be configured to a particular device, if needed. For details see the FactoryTalk Help:
Start > Programs > Rockwell Software > FactoryTalk Tools > FactoryTalk Help.

6. In the Logical Name list, select the Controller name. This name should match the settings from the Controller Properties dialog box made during the "Securing a Logix Designer Application Project File" section. The controller name can also be manually typed in if the name does not appear in the list.

IMPORTANT Security settings can be applied to a Logical Name. The Logical Name is the same as the *Name* shown on the Controller Properties dialog. Security settings for a Logical Name apply to the offline project, as well as when the project is downloaded to the controller.

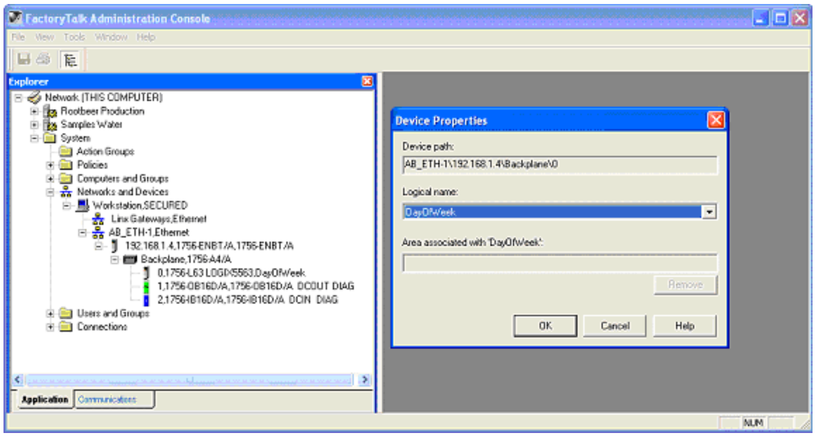
Security can be configured on a Logical Name associated to a particular device, and Logic Names can also be associated to an Application or Area in the FactoryTalk Explorer window. Security applied to an Application or Area is inherited by any Logical Names associated with that Application or Area. In the image in Step 5, *Rootbeer Production* and *Samples Water* are Applications, and an Area would be located below an Application. You right click on an Application or Area and use the Resource Editor to associate Logical Names to that Application or Area.

Security can also be configured at the Networks and Devices level in the Explorer window by right clicking and selecting **Security**. Security settings configured at the Networks and Devices level are inherited by all devices located under Networks and Devices. Security can be configured at the top-most node in the Explorer window, and all Applications, Areas, and devices will inherit these permissions.

TIP

- The controller in the Network and Devices tree will also display the controller name property next to the controller resource.
- If the name does not appear in the Network and Devices tree, open RSLinx Classic and navigate to the controller resource with RSWho. Navigating to the resource in RSLinx Classic will update the Controller path information in RSLinx Classic. FactoryTalk Administration Console uses the controller path information from RSLinx Classic to display Controllers. Once the path information is updated in RSLinx Classic, open the FactoryTalk Administration Console and right-click on the **Network and Devices** tree and select **Refresh**.

7. Click **OK** to continue.



Device path: AB_ETH-1\192.168.1.4\Backplane\0

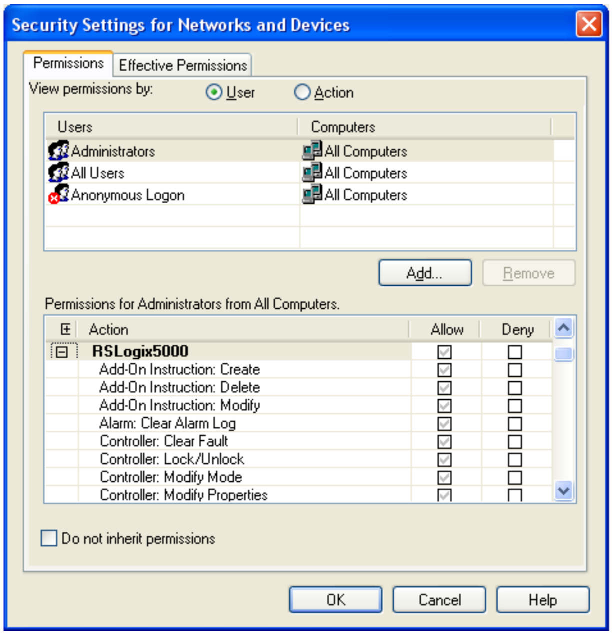
Logical name: DayOfWeek

Area associated with 'DayOfWeek':

8. Individual user or groups rights will still need to be configured to control access to secured controllers.

   To configure Security, right click on the Network, Networks and Devices, Application, Area, or the particular device on which you wish to configure security, then select **Security** from the menu.

9. From the Security Settings dialog, you can configure security permissions for a particular user or user group and computer names.



View permissions by: ● User ○ Action

Users	Computers
Administrators	All Computers
All Users	All Computers
Anonymous Logon	All Computers

Permissions for Administrators from All Computers.

Action	Allow	Deny
RSLogix5000	☑	□
Add-On Instruction: Create	☑	□
Add-On Instruction: Delete	☑	□
Add-On Instruction: Modify	☑	□
Alarm: Clear Alarm Log	☑	□
Controller: Clear Fault	☑	□
Controller: Lock/Unlock	☑	□
Controller: Modify Mode	☑	□
Controller: Modify Properties	☑	□

□ Do not inherit permissions

This completes the FactoryTalk Security configuration for a controller resource. For more FactoryTalk Security information, refer to the *FactoryTalk Security System Configuration Guide*, publication FTSEC-QS001.

Migrating from a Security Server Database to a FactoryTalk Server

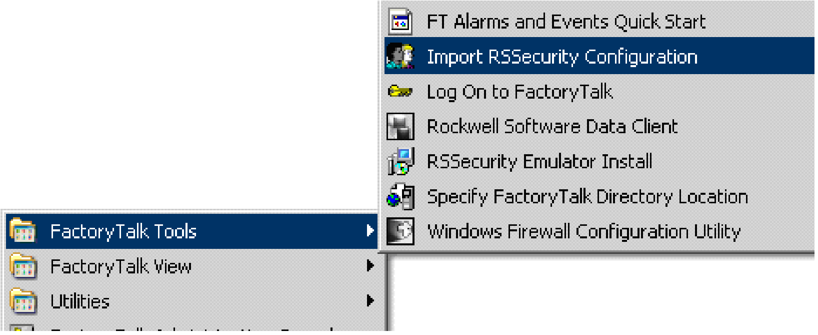
Introduction

To migrate to a FactoryTalk Security Server you must first export the security server database and then import the database into FactoryTalk.

Importing a Security Server Database

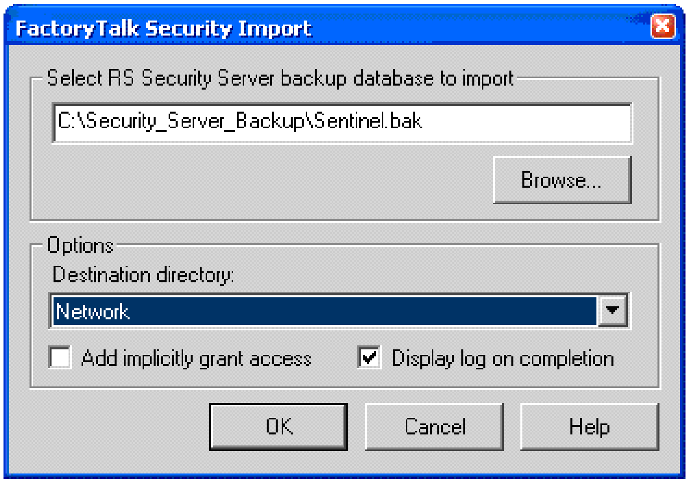
Follow these steps to import a security server database into FactoryTalk Security.

1. From the Start menu, select **Programs>Rockwell Software>FactoryTalk Tools>Import RSSecurity Configuration**


FT Alarms and Events Quick Start
Import RSSecurity Configuration
Log On to FactoryTalk
Rockwell Software Data Client
RSSecurity Emulator Install
Specify FactoryTalk Directory Location
Windows Firewall Configuration Utility
FactoryTalk Tools
FactoryTalk View
Utilities

2. Select **Import File**.

3. Browse to the import file and Destination directory from the menu.



FactoryTalk Security Import

Select RS Security Server backup database to import

C:\Security_Server_Backup\Sentinel.bak

Browse...

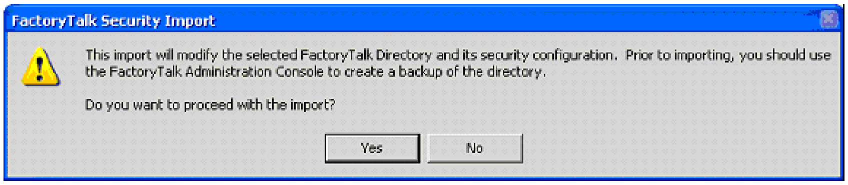
Options

Destination directory: Network

□ Add implicitly grant access ☑ Display log on completion

OK Cancel Help

4. Click **Yes** at the Warning message.

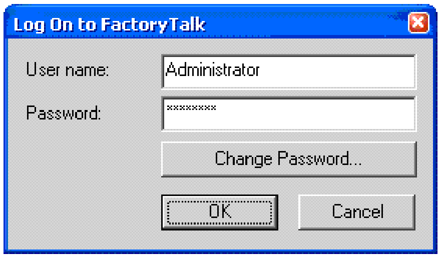


FactoryTalk Security Import

This import will modify the selected FactoryTalk Directory and its security configuration. Prior to importing, you should use the FactoryTalk Administration Console to create a backup of the directory.

Do you want to proceed with the import?

5. Type your user name and password and click **OK**.

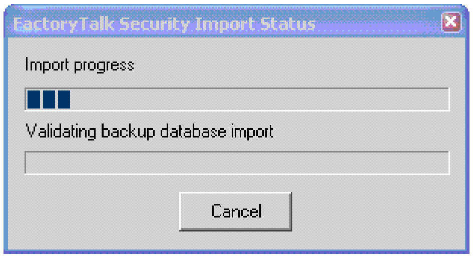


Log On to FactoryTalk

User name: Administrator

Password: ********

The import status appears.

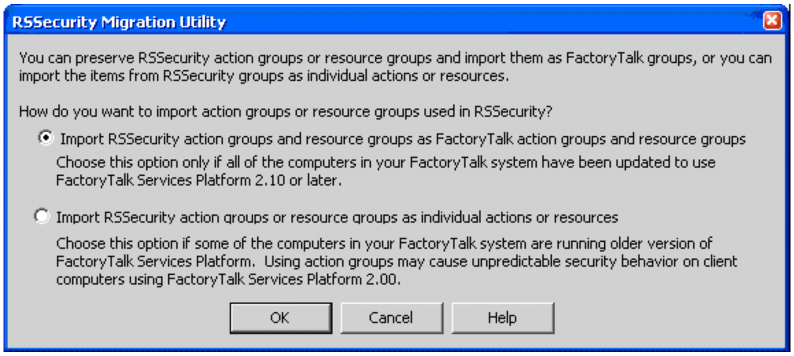


FactoryTalk Security Import Status

Import progress

Validating backup database import

6. Select how you want action and resource groups to be imported into FactoryTalk and click **OK**.



RSSecurity Migration Utility

You can preserve RSSecurity action groups or resource groups and import them as FactoryTalk groups, or you can import the items from RSSecurity groups as individual actions or resources.

How do you want to import action groups or resource groups used in RSSecurity?

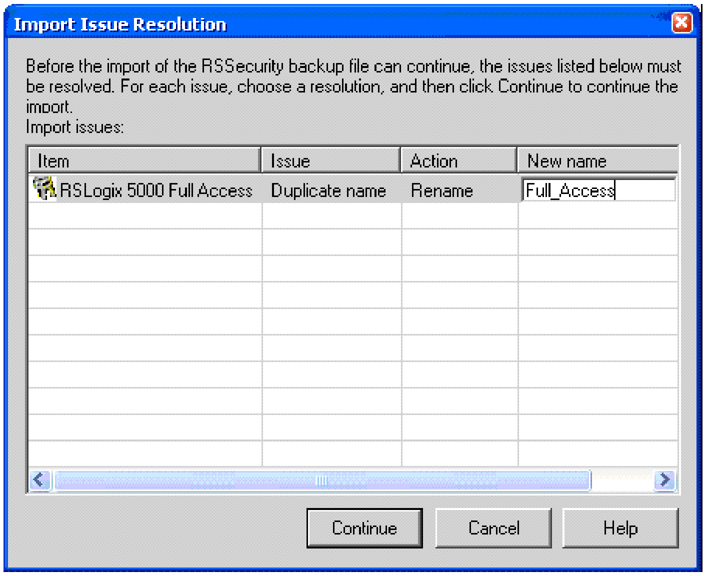
● Import RSSecurity action groups and resource groups as FactoryTalk action groups and resource groups

Choose this option only if all of the computers in your FactoryTalk system have been updated to use FactoryTalk Services Platform 2.10 or later.

○ Import RSSecurity action groups or resource groups as individual actions or resources

Choose this option if some of the computers in your FactoryTalk system are running older version of FactoryTalk Services Platform. Using action groups may cause unpredictable security behavior on client computers using FactoryTalk Services Platform 2.00.

7. Review the import issue resolution and click **Continue**.

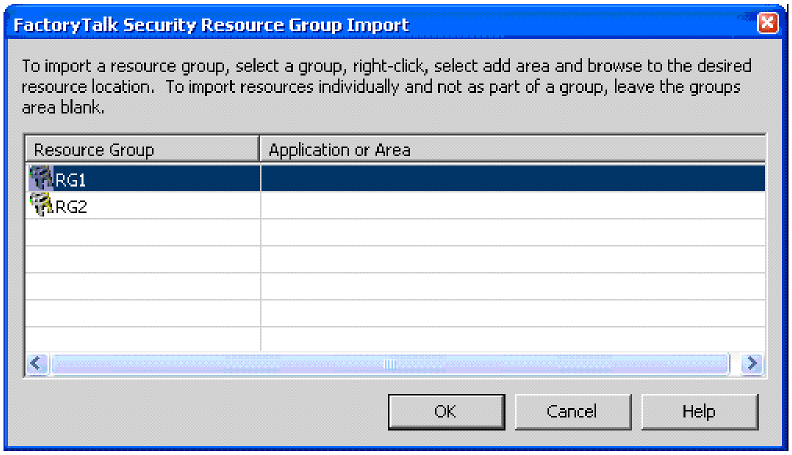


Import Issue Resolution

Before the import of the RSSecurity backup file can continue, the issues listed below must be resolved. For each issue, choose a resolution, and then click Continue to continue the import.
Import issues:

Item	Issue	Action	New name
RSLogix 5000 Full Access	Duplicate name	Rename	Full_Access

8. Select a group to import.



FactoryTalk Security Resource Group Import

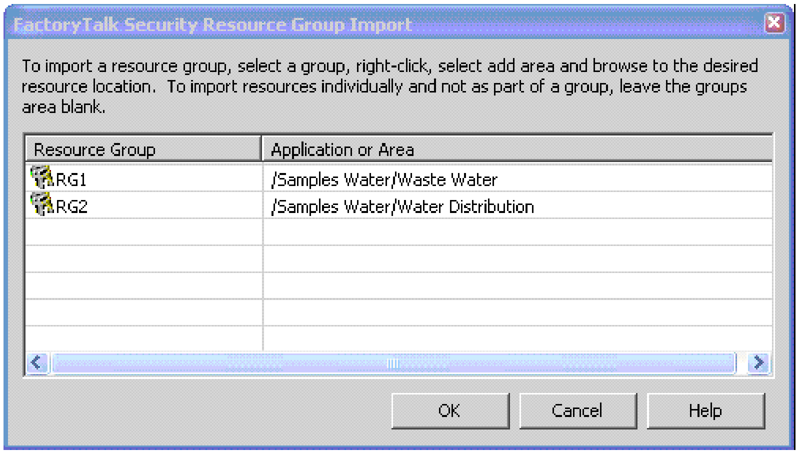
To import a resource group, select a group, right-click, select add area and browse to the desired resource location. To import resources individually and not as part of a group, leave the groups area blank.

Resource Group	Application or Area
RG1	
RG2	

9. Right-click the selected group, select **Add Area**, and browse to the resource location.

10. Click **OK**.

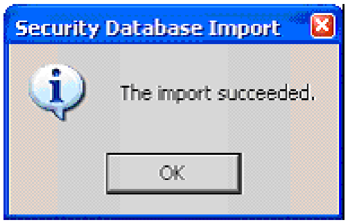
11. Click **OK**.



To import a resource group, select a group, right-click, select add area and browse to the desired resource location. To import resources individually and not as part of a group, leave the groups area blank.

Resource Group	Application or Area
RG1	/Samples Water/Waste Water
RG2	/Samples Water/Water Distribution

The import succeeded graphic appears.

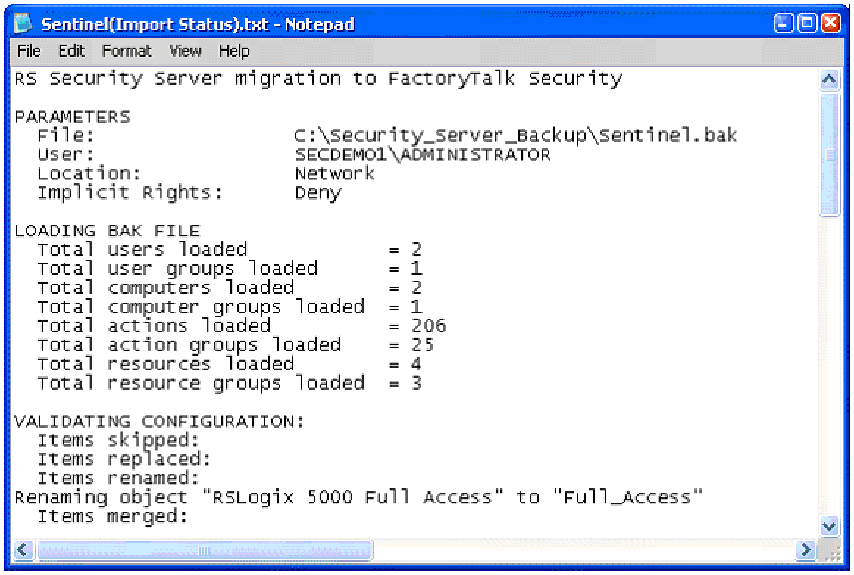


The import succeeded.

12. Click **OK**.

Importing Status Text File

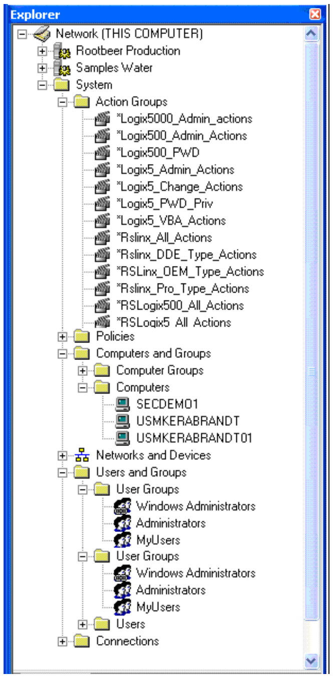
This graphic shows an example of the Import Status text file that is created when an import is completed.


Sentinel(Import Status).txt - Notepad
File Edit Format View Help

```
RS Security Server migration to FactoryTalk Security

PARAMETERS
  File:                   C:\Security_Server_Backup\Sentinel.bak
  User:                   SECDEMO1\ADMINISTRATOR
  Location:               Network
  Implicit Rights:        Deny

LOADING BAK FILE
  Total users loaded             = 2
  Total user groups loaded       = 1
  Total computers loaded         = 2
  Total computer groups loaded   = 1
  Total actions loaded           = 206
  Total action groups loaded     = 25
  Total resources loaded         = 4
  Total resource groups loaded   = 3

VALIDATING CONFIGURATION:
  Items skipped:
  Items replaced:
  Items renamed:
Renaming object "RSLogix 5000 Full Access" to "Full_Access"
  Items merged:
```

Organizer Import Result

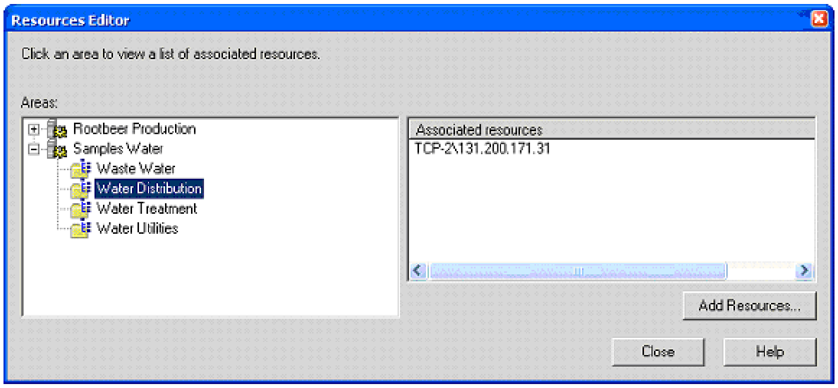
This graphic shows the results of the import process in the Organizer.



```
Network (THIS COMPUTER)
  Rootbeer Production
  Samples Water
  System
    Action Groups
      *Logix5000_Admin_actions
      *Logix500_Admin_Actions
      *Logix500_PWD
      *Logix5_Admin_Actions
      *Logix5_Change_Actions
      *Logix5_PWD_Priv
      *Logix5_VBA_Actions
      *Rslinx_All_Actions
      *Rslinx_DDE_Type_Actions
      *RSLinx_OEM_Type_Actions
      *Rslinx_Pro_Type_Actions
      *RSLogix500_All_Actions
      *RSLogix5_All_Actions
    Policies
    Computers and Groups
      Computer Groups
      Computers
        SECDEMO1
        USMKERABRANDT
        USMKERABRANDT01
    Networks and Devices
    Users and Groups
      User Groups
        Windows Administrators
        Administrators
        MyUsers
      User Groups
        Windows Administrators
        Administrators
        MyUsers
      Users
    Connections
```

Resource Editor

This graphic shows the results of the import in the Resource Editor.



Resources Editor

Click an area to view a list of associated resources.

Areas:

- Rootbeer Production
- Samples Water
  - Waste Water
  - Water Distribution
  - Water Treatment
  - Water Utilities

Associated resources

TCP-2\131.200.171.31

Configuring Source Protection in the Logix Designer Application

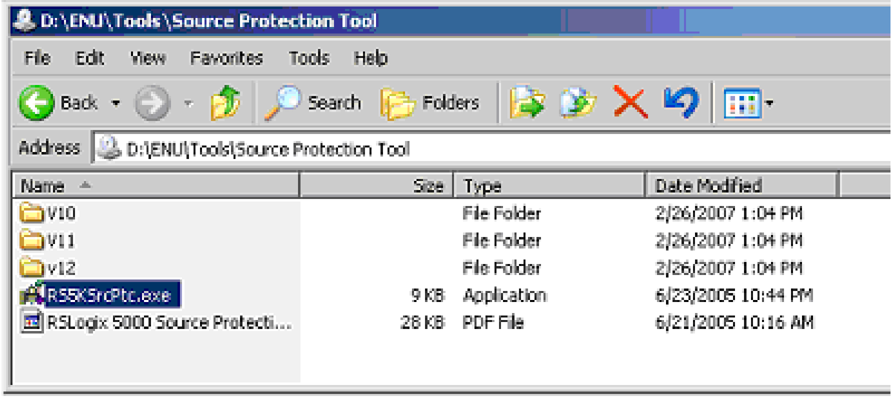
Introduction

This chapter describes how to enable and apply source protection for your Logix Designer components such as routines and Add-On Instructions.

Enabling Source Protection

Do these steps to enable Logix Designer source protection.

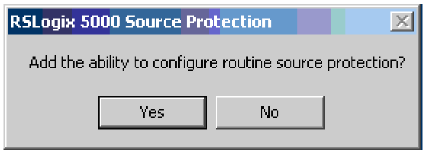
1. On the Logix Designer installation CD, browse to **D:\ENU\Tools\Source Protection Tool** and double-click on the **RS5KSrcPtc.exe**.



D:\ENU\Tools\Source Protection Tool

Name	Size	Type	Date Modified
V10		File Folder	2/26/2007 1:04 PM
V11		File Folder	2/26/2007 1:04 PM
v12		File Folder	2/26/2007 1:04 PM
RS5KSrcPtc.exe	9 KB	Application	6/23/2005 10:44 PM
RSLogix 5000 Source Protecti...	28 KB	PDF File	6/21/2005 10:16 AM

A dialog box appears.


RSLogix 5000 Source Protection

Add the ability to configure routine source protection?

2. Click **Yes**.

Applying Source Protection

This procedure lets you apply source protection to a project file. When a source key is applied to a component, that component is source-protected. Source keys are user-generated, case-sensitive passwords that lock Logix Designer components from being viewed or modified by third parties.

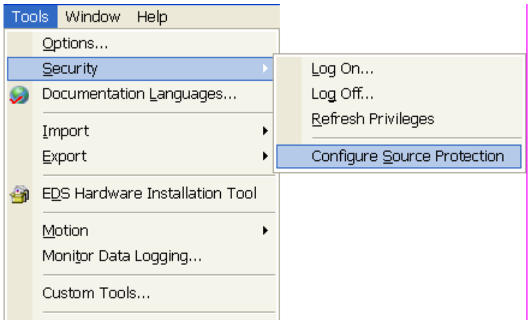
IMPORTANT Source Protection can be applied only on a project file that is offline.

Specifying a Source Key File

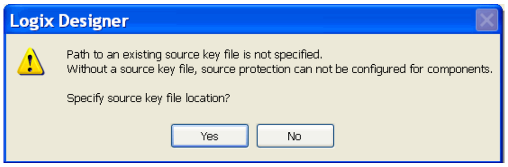
Do these steps to configure a file location.

1. Open an offline project file.
2. From the Tools menu, click **Tools** and choose **Configure Source Protection**.

TIP This menu option is not available until you have run RS5KSrcPtc.exe on your workstation.



Source Protection requires a Source Key File location to be specified on your workstation. You are prompted to configure a file location.

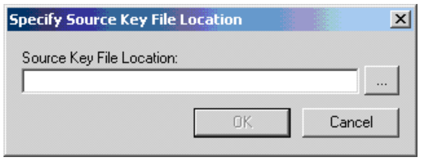


Path to an existing source key file is not specified.
Without a source key file, source protection can not be configured for components.

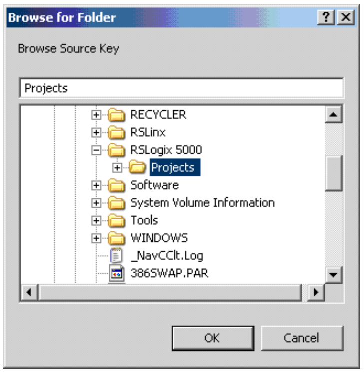
Specify source key file location?

3. Click **Yes**.

4. Click Browse ... to specify a Source Key File location.



5. Navigate to the folder location to store the Key File.

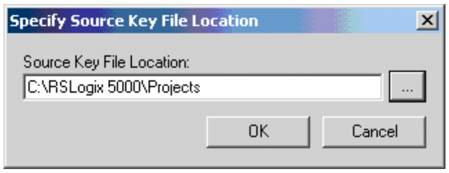


Browse Source Key

Projects

The key file can be saved in any accessible folder. In this example, **C:\RSLogix 5000\Projects folder** is specified as the Key File location.

6. Click **OK** to continue.

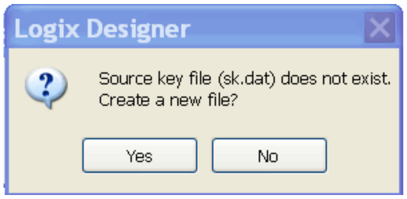


Source Key File Location: C:\RSLogix 5000\Projects

Once you return to the Source Protection Configuration dialog box, the location you selected appears under Source Key Provider.

If a Key File is not found in the specified location, you will be prompted to create a new Key File.

TIP To check for a specific location, click the **Specify** button on the Source Protection Configuration dialog box. A window appears with the location, if one exists on your workstation.

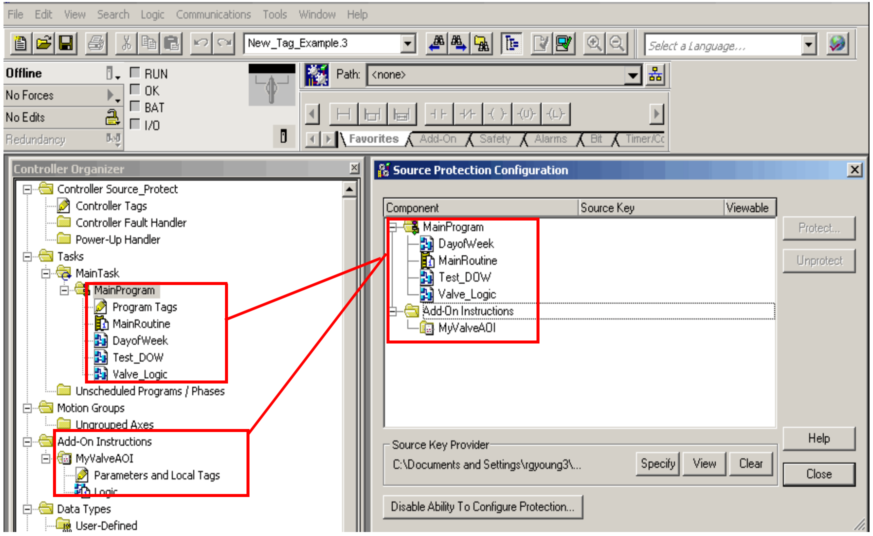


Source key file (sk.dat) does not exist.
Create a new file?

7. Click **Yes** to create a new key file.

Protecting Components

The Source Protection Configuration dialog box lists all Program Routines, Add-On Instructions, and Equipment Phase State Routines in the project file. These components are protected by applying source keys to them. Source keys are user-generated passwords used to lock components. Users that do not have the source key for a component are not able to modify the component and may not be able to view the component.



About Source Keys

In version 18 and earlier of RSLogix 5000 software, only IEC-61131 compliant source keys are recognized. Each source key must begin with a lowercase character a-z or underscore character (_), and contain only characters lowercase a-z, 0-9, and an underscore character (_). Uppercase A-Z may be entered in RSLogix 5000 software or in the source key file, but the uppercase characters will be converted to lowercase. Source keys are limited to 40 characters in length.

In version 19 and later of the application, source keys are case-sensitive and may contain any printable ASCII character, excluding the space character. This includes uppercase A-Z, lowercase a-z, numbers 0-9, and symbols such as "!@#$%. Source keys are limited to 40 characters in length.

Source Key Names

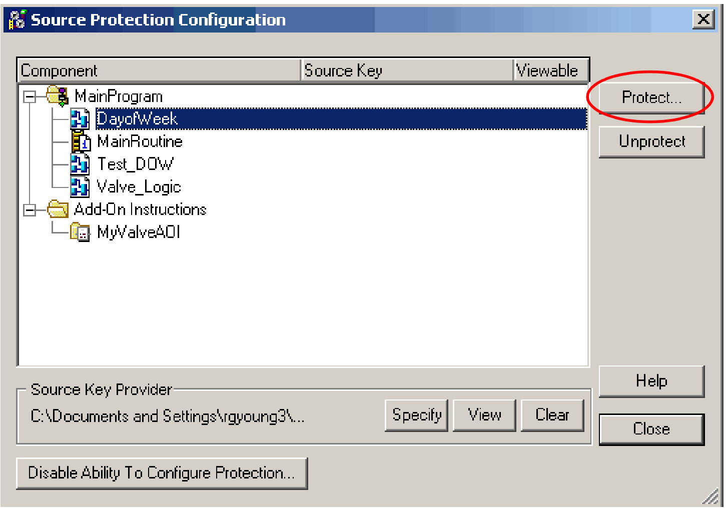
Version 19 and later of the application supports associating names with source keys. Source key names are descriptive text that help identify source keys. Where appropriate, Logix Designer application will display the source key name in place of the source key itself. This provides an additional layer of security for the source key.

Descriptive names should be used to help identify the purpose of the source. For instance, a source key used to secure components that field engineers require access might be named, *Field Engineer*.

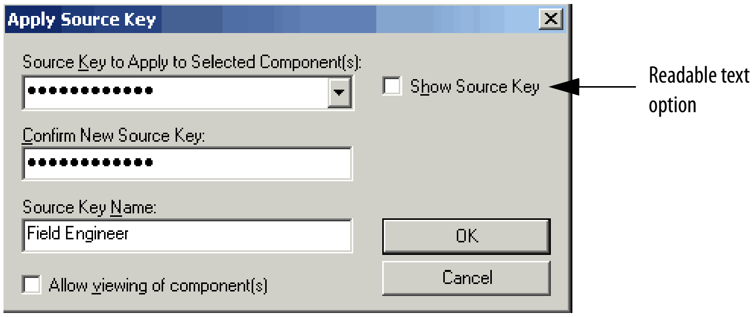
IMPORTANT	If the same source keys will be used with version 18 and earlier and version 19 and later of the application, begin each source key with a lowercase character a-z, or an underscore character (_), and use only characters lowercase a-z, 0-9 , or an underscore character (_) within the source keys. If you use source key names in version 19 and later of the application, and your source keys are IEC61131-3 compliant, your source keys will still work in version 18 and earlier.

Do these steps to apply a source key to one or more components.

1. Select one or more components that require protection and click **Protect**.



The Apply Source Key dialog box appears.



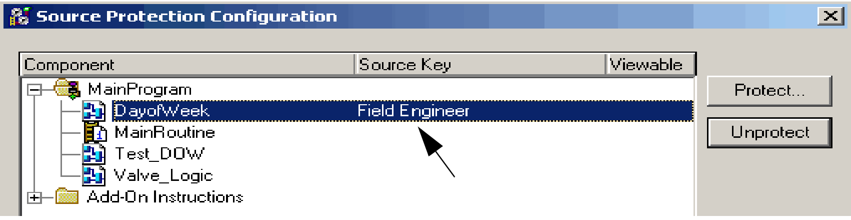
For version 19 and later of the application, the entered source keys on the Apply Source Key dialog box are masked by default, but you have an option to display readable text. If you have version 18 and earlier of RSLogix 5000 software, your source keys are in a readable, text-only format.

2. Complete the Apply Source Key dialog box to designate a new source key.

Element	Description
Source Key to Apply to Selected Component(s)	Type a new key. Source keys cannot exceed 40 characters. The Confirm New Source Key and Source Key Name boxes become active for version 19 and later of the application. To select an existing key, click the down arrow. When the source key is selected, the Confirm New Source Key and Source Key Names boxes become read-only. The Confirm New Source Key box will be empty, and the Source Key Name box will contain the name of the selected source key, if one exists.
Show Source Key	For version 19 and later of the application, click the check box to display source keys in a readable format.
Confirm New Source Key	Re-type exactly the characters you typed in the Source Key to Apply to Selected Component(s) field. This box is unavailable when an existing source key is selected or when the source key is being displayed in cleartext.
Source Key Name	Type a name for the source key; do not exceed 40 characters. The box displays the name of a selected, existing source key, if one is defined.
Allow viewing of component(s)	You can set a protected routine to allow or deny viewing of the routine from a system that does not have the key required to access the routine. Select the check box to allow viewing of a routine in read-only mode. Protected routines that do not allow viewing cannot be viewed by systems that do not have the required key.

3. Click **OK**.

The Source Protection Configuration dialog box reappears.



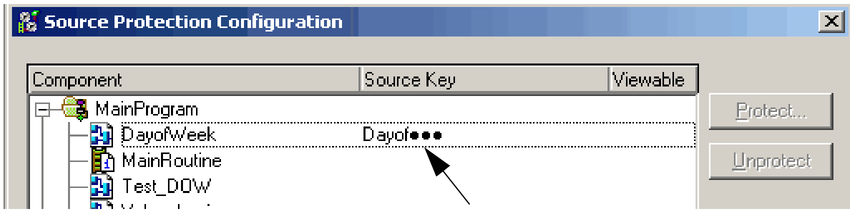
Component	Source Key	Viewable
MainProgram		
DayofWeek	Field Engineer	
MainRoutine		
Test_DOW		
Valve_Logic		
Add-On Instructions		

For version 19 and later of the application, source keys may have names. Where appropriate, the source key name is displayed instead of the source key. This further protects the source key from being seen.

In the example, the name *Field Engineer* is displayed instead of a source key.

IMPORTANT	Source key names cannot be added to existing source keys through the Logix Designer application. See page 40 to learn how to associate a name to an existing source key.

For version 19 and later of the application, unnamed source keys are obfuscated. Three black circles appear after the last character or any character beyond the fifth character to provide security.


Source Protection Configuration

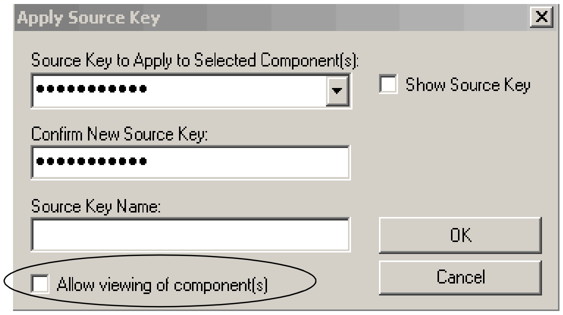
Component	Source Key	Viewable
MainProgram		
DayofWeek	Dayof●●●	
MainRoutine		
Test_DOW		

4. Close the Source Protection Configuration dialog box and save the project file.

Viewing Components Without a Key

This procedure lets you flag source-protected components to be available in a read-only format on a system that does not have the source keys.

1. Enter a source key on the Apply Source Key dialog box.


Apply Source Key

Source Key to Apply to Selected Component(s): ●●●●●●●●●●●

□ Show Source Key

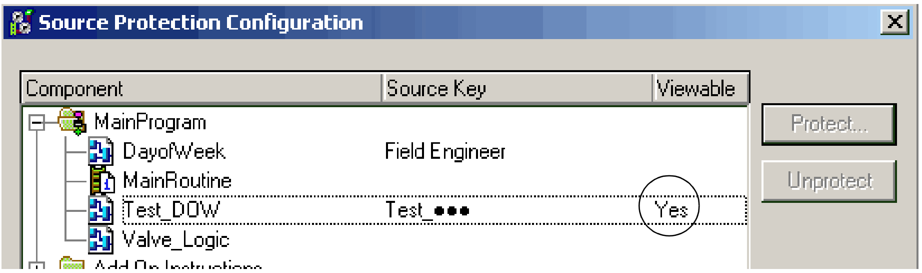
Confirm New Source Key: ●●●●●●●●●●●

Source Key Name:

□ Allow viewing of component(s)

2. (optional) Name the source key.
3. Select the **Allow viewing of components** check box.
4. Click **OK**.

   The Test_DOW routine in the example is source-protected and can be viewed (as indicated by *Yes*) in a read-only format on workstations that do not have the source key.


Source Protection Configuration

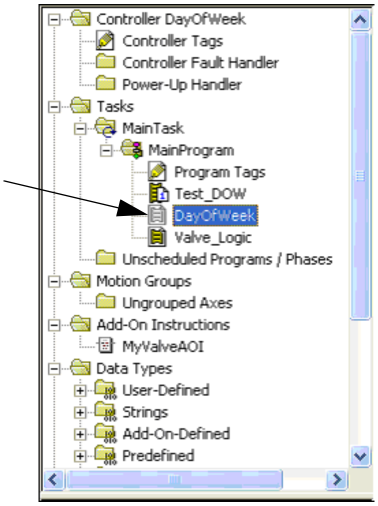
Component	Source Key	Viewable
MainProgram		
DayofWeek	Field Engineer	
MainRoutine		
Test_DOW	Test_●●●	Yes
Valve_Logic		
Add On Instructions		

5. Click **Close**.
6. Save the project file and download it to the controller.

When the project file is opened on a system that does not contain the keys used to secure the routines and Add-On Instructions, the components will be protected based on the setting in the Source Protection Configuration dialog box.

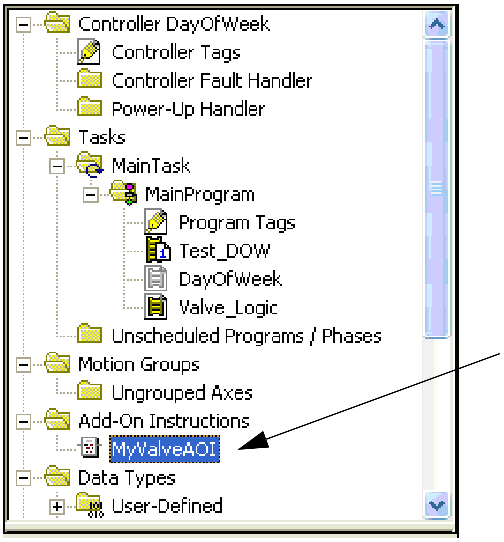
Test_DOW was protected and set to viewable on the Source Protection Configuration dialog box. You can open the routine as read-only on a system that does not contain the key for the routine, but you will not be able to modify the routine.

Routines or Add-On Instructions that are protected, but are not configured as viewable, cannot be opened. The Dayof Week routine cannot be opened on a system that does not have the key used to protect the routine. In the example, the icon for the routine is dimmed, indicating the routine cannot be opened.



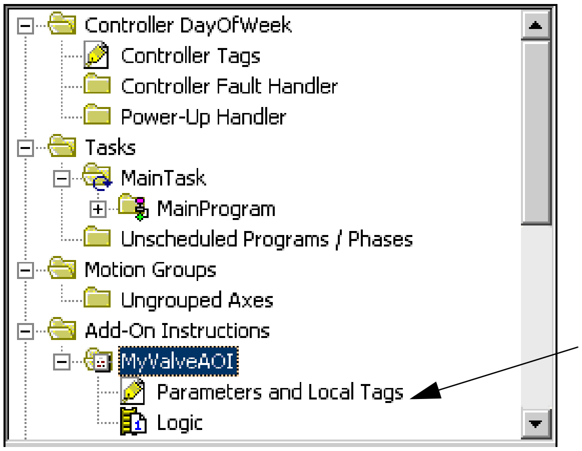
Inactive icons are dimmed.

The MyValveAOI cannot be viewed on a system that does not contain the key used to protect the Add-On Instruction. This is because MyValveAOI was protected, but not set to be viewable. The Add-On Instruction is shown in the Controller Organizer, but the parameters and local tags for the Add-On Instructions are not viewable on a system that does not contain the required key used to protect it.



Local Tags and Logic are not viewable. Parameters can be viewed but not edited.

This example shows the Add-On Instruction MyValveAOI viewed from a system that has the key used to secure the instruction.



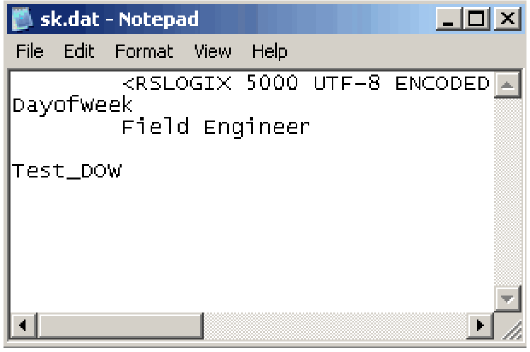
Parameters, Local Tags, and Logic are viewable and can be edited.

TIP For source-protected export options, see the *Logix5000 Controllers Import/Export Reference Manual*, publication 1756-RM084.

Source-protected content cannot be copied from version 19 of RSLogix 5000 software and pasted into earlier software versions. The pasting function will be disabled in previous software versions when source-protected content is placed on the clipboard.

Source Key File

Source keys made available to the application through an sk.dat file are unencrypted. We recommend that you back up and store the key in a secure location. If necessary, the individual keys can be distributed or provided to the necessary parties.



```
        <RSLOGIX 5000 UTF-8 ENCODED
DayofWeek
        Field Engineer

Test_DOW
```

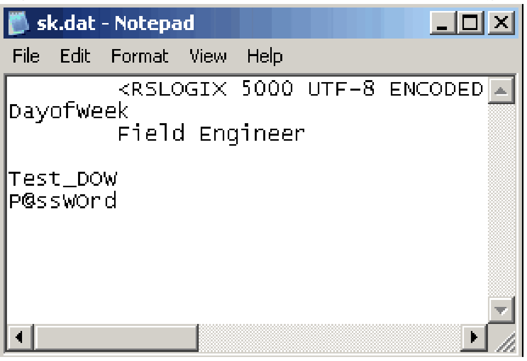
Text must be in first line.

IMPORTANT Source key files are created in an ANSI format in RSLogix 5000 software version 18 and earlier. Software version 19, and later, creates UTF-8 formatted sk.dat files. ANSI sk.dat files modified in software version 19, and later, are converted to UTF-8 sk.dat files.

Source keys **must not** appear on the first line of a UTF-8 formatted sk.dat file. The first line of UTF-8 formatted sk.dat files is ignored by RSLogix 5000 software version 18 and earlier. Versions 19 and later insert a header on the first line of the sk.dat file if one is not already present.

Do these steps to assign a name to an existing source key.

1. Close the Logix Designer application.
2. Locate the sk.dat file on your workstation.
3. Open the file with a text editor, such as Notepad or WordPad.



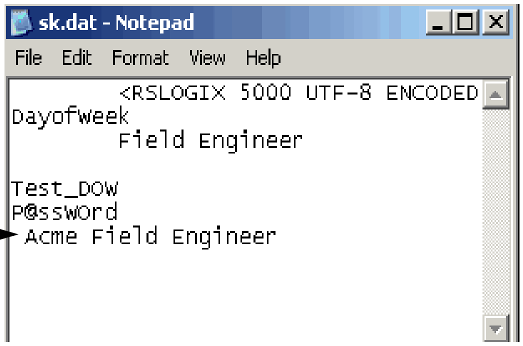
```
        <RSLOGIX 5000 UTF-8 ENCODED
DayofWeek
        Field Engineer

Test_DOW
P@ssWOrd
```

4. Click the mouse at the end of an existing source key and press **Enter**.

   Note that our example, P@ssWOrd, shows that source keys are case sensitive and may use special characters like @#$%(){}[].

5. Click the space bar once and type a name for the source key.

One or more character of white space is required to associate the name with the source key.



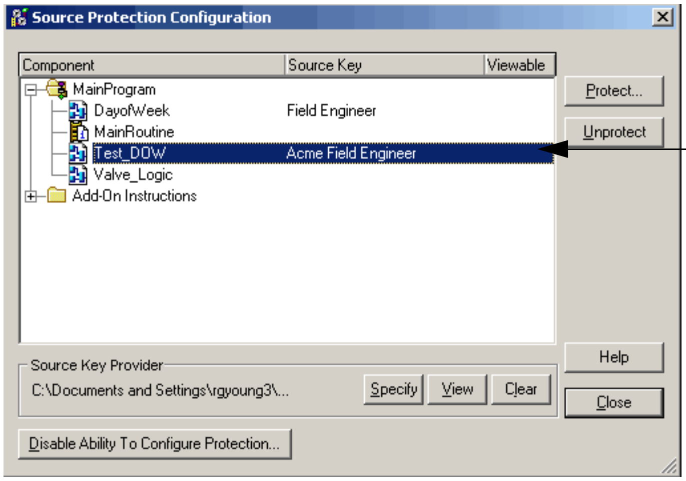
```
        <RSLOGIX 5000 UTF-8 ENCODED
DayofWeek
        Field Engineer

Test_DOW
P@ssWOrd
 Acme Field Engineer
```

One character space for source key names

Source keys always begin in the first character of the text editor. A source key name must be on the line immediately following the source key that it is associated with, and at least one character of white space. Subsequent lines after the source key that are preceded with white space are ignored by the application, and can be used for comments.

6. Choose **File>Save**.
7. Open the Logix Designer application.
8. Choose **Tools>Configure Source Protection**.

Acme Field Engineer replaces *P@ssWOrd* in the Source Key column on the Source Protection Configuration dialog box.

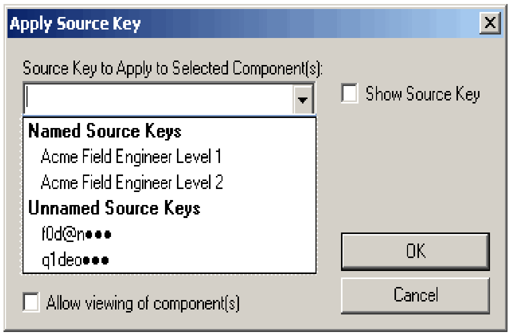

Source Protection Configuration
Protect...
Unprotect
Help
Close
Specify
View
Clear
Disable Ability To Configure Protection...

Component	Source Key	Viewable
MainProgram		
DayofWeek	Field Engineer	
MainRoutine		
Test_DOW	Acme Field Engineer	
Valve_Logic		
Add-On Instructions		

Source Key Provider
C:\Documents and Settings\rgyoung3\...

9. To use the named source key, select the component that you gave a name and click **Protect**.

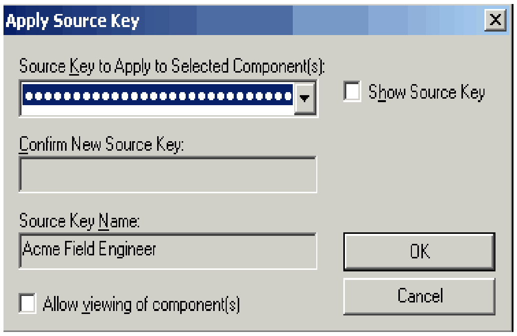
The Apply Source Key dialog box displays.


Apply Source Key
Source Key to Apply to Selected Component(s):
□ Show Source Key
OK
Cancel
□ Allow viewing of component(s)

Named Source Keys
Acme Field Engineer Level 1
Acme Field Engineer Level 2
Unnamed Source Keys
f0d@n●●●
q1deo●●●

10. Click the pull-down in the first entry box, and select the name you associated with the source key.

    The source key that is masked for privacy appears and the name is in the Source Key Name box.



Source Key to Apply to Selected Component(s): ●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Source Key Name: Acme Field Engineer

11. Click **OK**.

Verifying Source Protection on a Component

Make a decision on what method you want to use to see how a component looks when it is source protected and when it is not.

When the Source Key is available, the component behaves the same as if it were not source protected. To verify source protection, you remove the source keys.

Here are a few ways to verify that your content is protected.

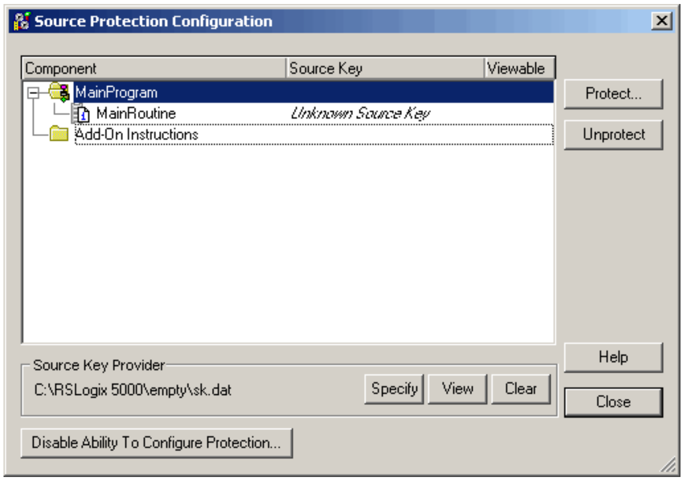
IMPORTANT	Disabling source protection using the RS5KSrcPT.exe tool does not remove the sk.dat file.

- Specify the path to a different sk.dat file
- Use buttons on the Source Protection Configuration dialog box

Specifying the Path to a Different sk.dat File

To use the specify path method, follow these steps.

1. On the Source Protection Configuration dialog box, click **Specify**.



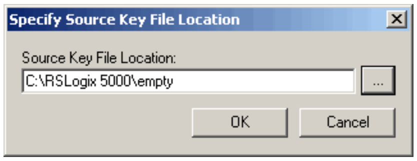
Source Protection Configuration

Component	Source Key	Viewable
MainProgram		
MainRoutine	*Unknown Source Key*	
Add-On Instructions		

Source Key Provider

C:\RSLogix 5000\empty\sk.dat

2. On the Specify Source Key File Location dialog box, select a directory that does not contain an sk.dat file. For example, **C:\RSLogix 5000\Projects\Empty.**



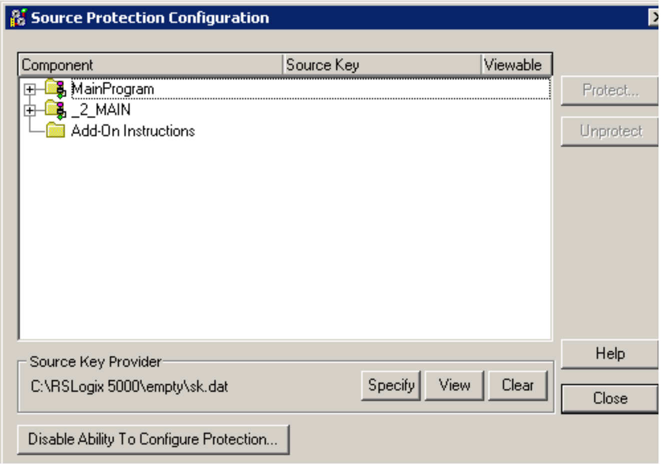
Specify Source Key File Location

Source Key File Location: C:\RSLogix 5000\empty

3. When the message appears and asks if you want to create a new file, click **Yes**.

4. When the message appears and asks if you want to create a new directory, click **Yes**.

The software now points to an empty sk.dat file which mimics a user who does not have a source key.



Advantage

Keeping an empty source key file around makes it easy to quickly switch back and forth between sk.dat files.

Disadvantage

Care must be taken that the correct sk.dat file is specified when creating new source keys.

Use the Clear Button

IMPORTANT Back up your sk.dat file before using this button.

On the Source Protection Configuration dialog box, the Clear button clears the location bar and gives you the option to delete your sk.dat file. See the steps under "Removing Access to a Protected Routine" on page 46.

Advantage

You can clear the location without removing the sk.dat file.

Disadvantages

If you delete the sk.dat, it will be erased. You need to make a backup file.

The sk.dat file is still present on the system under its original name and could be discovered.

Using the Disable Ability to Configure Source Protection Button

IMPORTANT	Back up your sk.dat file before using this button.

On the Source Protection Configuration dialog box, the Disable Ability to Configure Source Protection button deletes your sk.dat file. See the steps under "Disabling Routine Source Protection” on page 47.

Disadvantages

If you delete the sk.dat, it will be erased. You need to make a backup file.

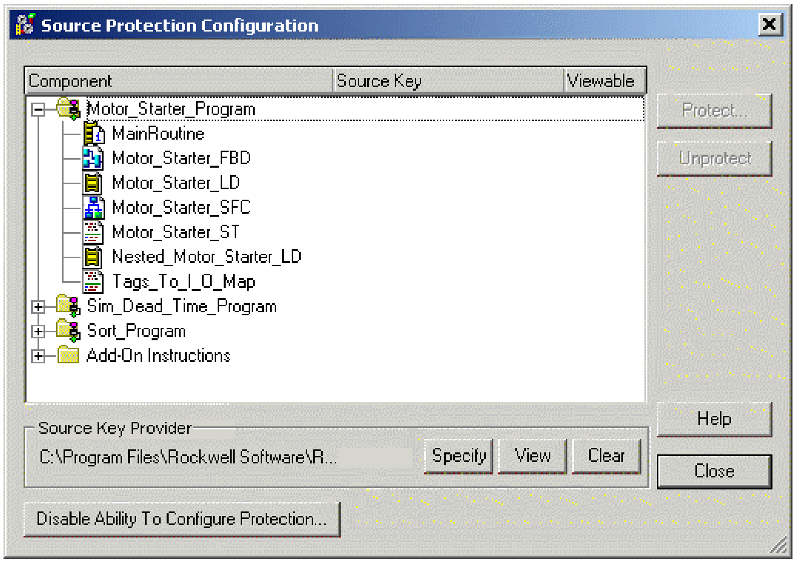
It requires that you re-enable source protection for the Source Protection option to be available under the Tools menu.

You can also rename or remove the sk.dat file to verify source protection, but you must make a backup file before you do so.

Removing Access to a Protected Routine

Before you remove a source key file (sk.dat) from a workstation, write down the source keys or make a copy of the file and store in a secure location.

1. Open the project that is protected.
2. From the Tools menu, choose **Security>Configure Source Protection**.



Source Key Provider: C:\Program Files\Rockwell Software\R...

3. Click **Clear**.

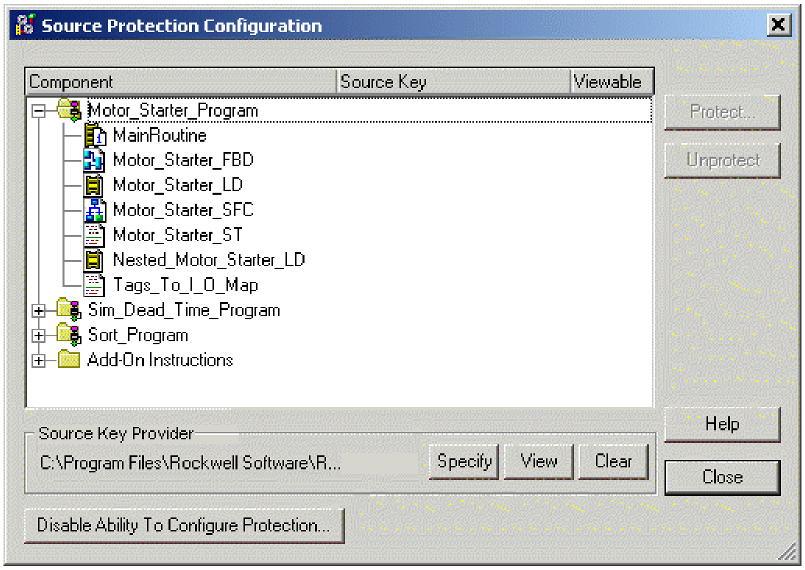
   A dialog box asks if you want to delete the source key file (sk.dat).

4. Select **Yes** to remove, or **No** not to remove the source key file from the workstation.

Disabling Routine Source Protection

Before you disable a source key file (sk.dat) from a workstation, write down the source keys or make a copy of the file and store in a secure location.

1. Open the project that is protected.
2. From the Tools menu, choose **Security>Configure Source Protection**.



3. Click the **Disable Ability To Configure Protection** button.

   A dialog box prompts you to confirm the action.

4. Click **Yes**.

   A dialog box asks if you want to delete the source key file (sk.dat).

5. Select **Yes** to remove the source key file from the computer or select **No** to retain the source key file.

Notes:

RSLogix 5000 Software CPU Security Tool

Introduction

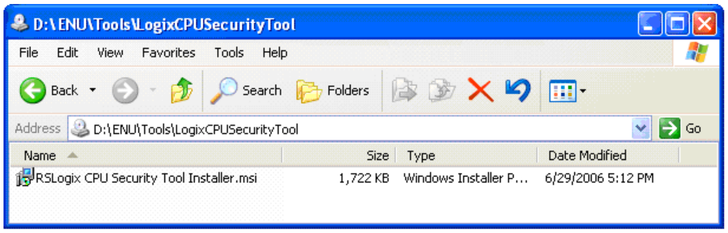
This chapter describes how to use the RSLogix 5000 CPU Security Tool to lock a controller. When a controller is locked, no one can access until it is unlocked.

Installation

The Logix CPU Security Tool is automatically installed when you install version 17 or later of the application. If you find that it is not installed, follow these installation instructions. The installation file is on the installation CD under the Tools folder.

Do these steps to install the Logix CPU Security Tool.

1. On the RSLogix 5000 installation CD, browse to **D:\ENU\Tools\LogixCPUSecurityTool** and double-click the RSLogix CPU Security Tool Installer.msi file.



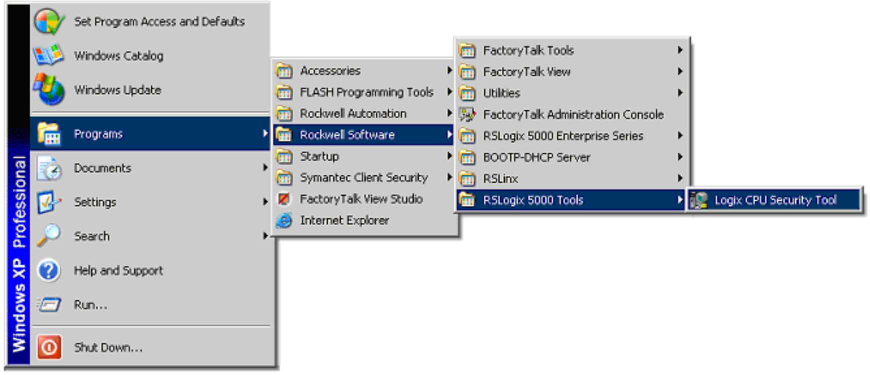
Address: D:\ENU\Tools\LogixCPUSecurityTool

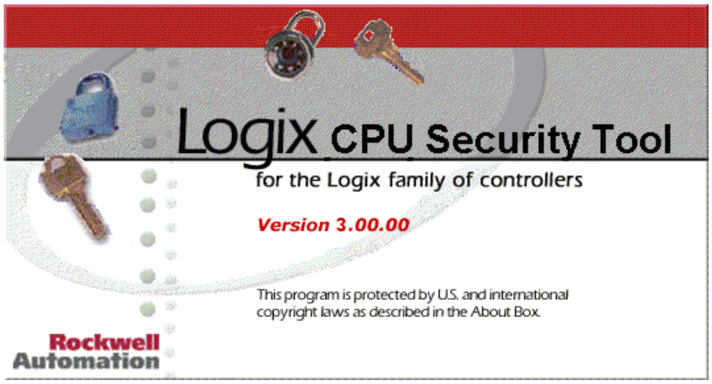
Name	Size	Type	Date Modified
RSLogix CPU Security Tool Installer.msi	1,722 KB	Windows Installer P...	6/29/2006 5:12 PM

2. Follow the installation prompts to complete the installation.

Securing a ControlLogix Controller with Logix CPU Security Tool

You can secure a controller with the Logix CPU Security Tool. The tool is installed under the Logix Desiger Tools menu.





Logix CPU Security Tool

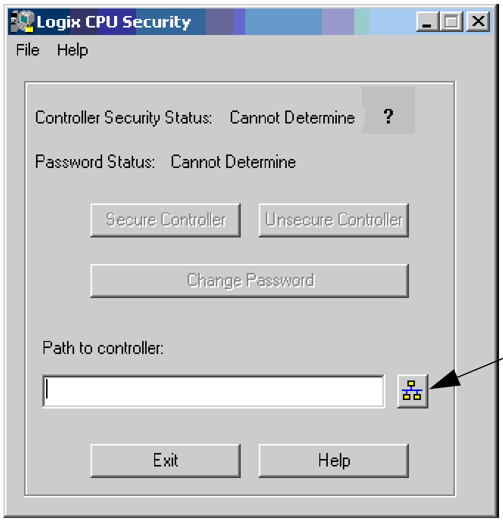
for the Logix family of controllers

Version 3.00.00

This program is protected by U.S. and international copyright laws as described in the About Box.

Rockwell Automation

1. Start the Logix CPU Security Tool.
2. To specify a path to the controller, click the RSWho button.



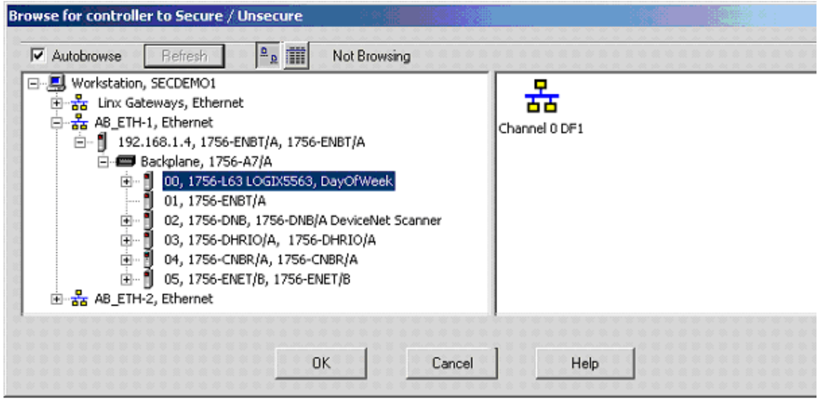
Controller Security Status: Cannot Determine

Password Status: Cannot Determine

Path to controller:

Use the RSWho button to locate the controller that you want to secure.

3. Select the controller that you want to secure and click **OK**.



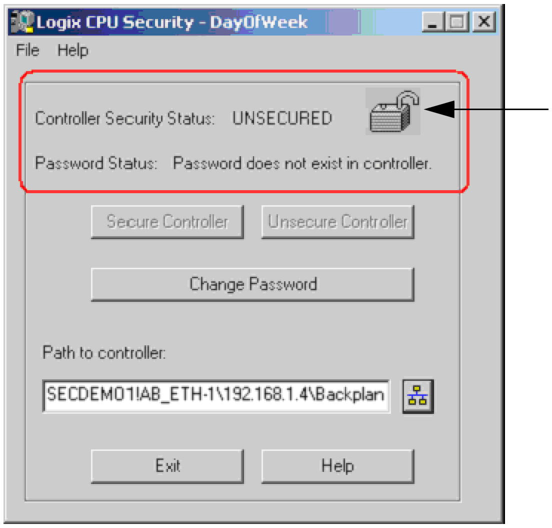
Browse for controller to Secure / Unsecure

☑ Autobrowse

Not Browsing

```
⊟ Workstation, SECDEMO1
   ⊞ Linx Gateways, Ethernet
   ⊟ AB_ETH-1, Ethernet
      ⊟ 192.168.1.4, 1756-ENBT/A, 1756-ENBT/A
         ⊟ Backplane, 1756-A7/A
            ⊞ 00, 1756-L63 LOGIX5563, DayOfWeek
              01, 1756-ENBT/A
            ⊞ 02, 1756-DNB, 1756-DNB/A DeviceNet Scanner
            ⊞ 03, 1756-DHRIO/A, 1756-DHRIO/A
            ⊞ 04, 1756-CNBR/A, 1756-CNBR/A
            ⊞ 05, 1756-ENET/B, 1756-ENET/B
   ⊞ AB_ETH-2, Ethernet
```

The Logix CPU Security Tool displays the current status of the controller.



Logix CPU Security - DayOfWeek

Controller Security Status: UNSECURED

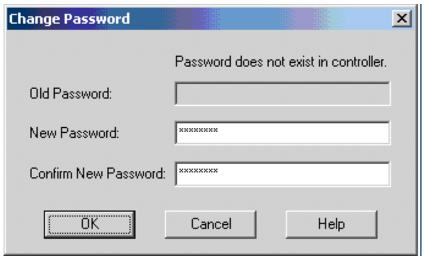
Password Status: Password does not exist in controller.

Path to controller: SECDEMO1!AB_ETH-1\192.168.1.4\Backplan

Notice that the controller you selected is currently unsecured and there is no password set in the controller.

4. Click **Change Password**.

5. Enter a password in the new password field and confirm the password and click **OK**.



Change Password

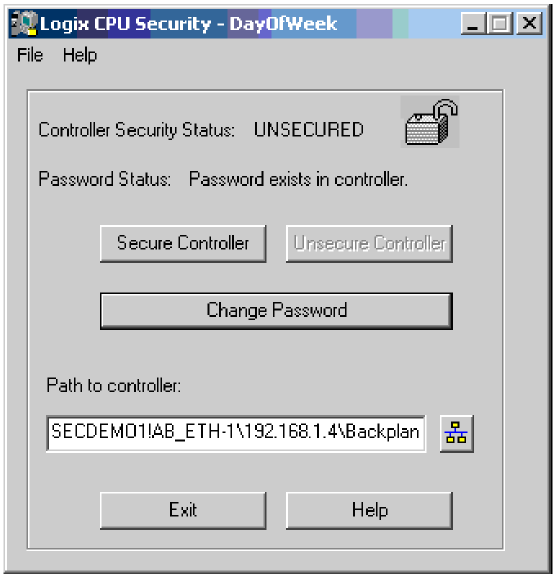
Password does not exist in controller.

Old Password:

New Password: ********

Confirm New Password: ********

The Password Status for the controller now indicates a Password exists in the controller, but the controller is not secured yet.



Controller Security Status: UNSECURED

Password Status: Password exists in controller.

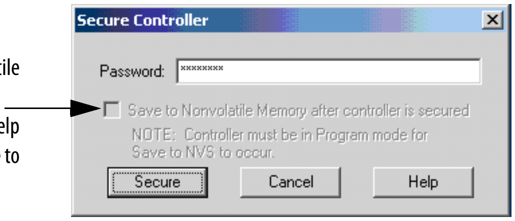
Path to controller:

SECDEMO1!AB_ETH-1\192.168.1.4\Backplan

6. Click **Secure Controller**.

7. Enter the password for the controller and click **Secure**.

If the controller has Nonvolatile Memory installed, this check box would save the security state of the controller to Nonvolatile Memory.
Refer to the Logix Designer Application Help for additional information on how to Save to Nonvolatile Memory.

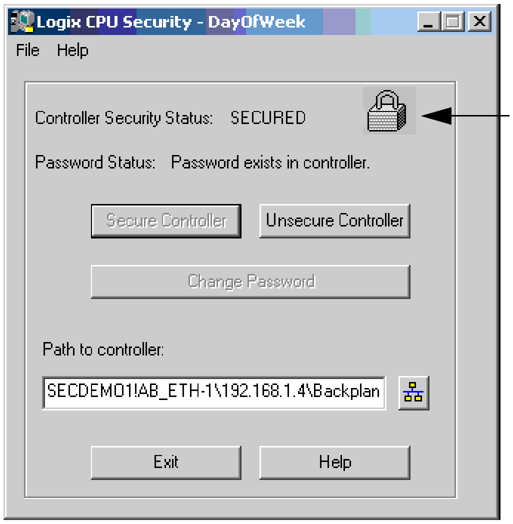


Password: *********

☐ Save to Nonvolatile Memory after controller is secured

NOTE: Controller must be in Program mode for Save to NVS to occur.

The controller is now secured.



Controller Security Status: SECURED

Password Status: Password exists in controller.

Path to controller:

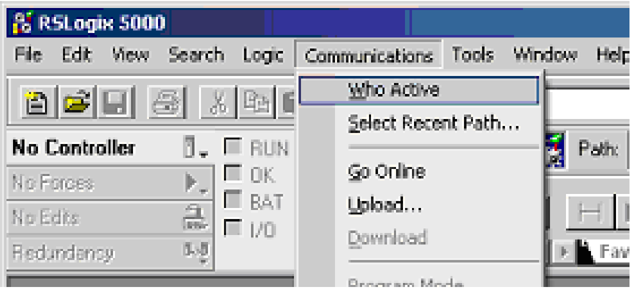
SECDEMO1!AB_ETH-1\192.168.1.4\Backplan

Accessing a Secured Controller

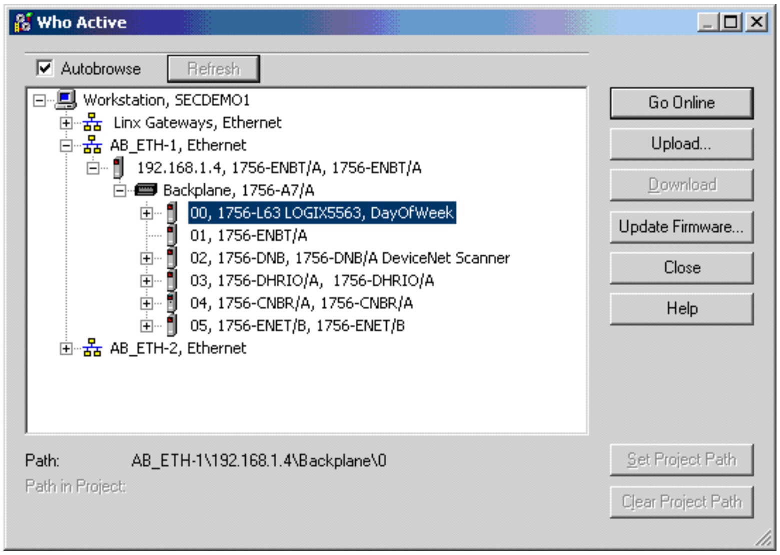
When you try to access a controller that has been secured by the Logix CPU Security Tool and you do not have a local copy of the project file on your computer, you will be prompted to select the proper file.

To access a secured controller, do the following.

1. From the Communications menu, select **Who Active**.



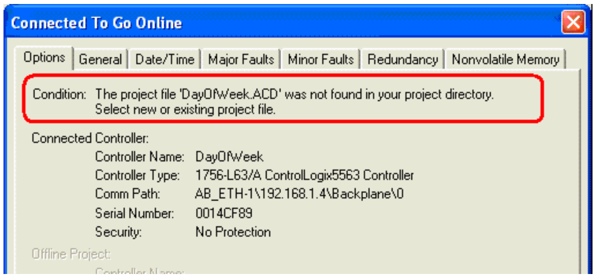
2. Select the secured controller and click **Go Online**.



Path: AB_ETH-1\192.168.1.4\Backplane\0

Path in Project:

If you do not have a local copy of the project file on your computer, you will be prompted to select a file.

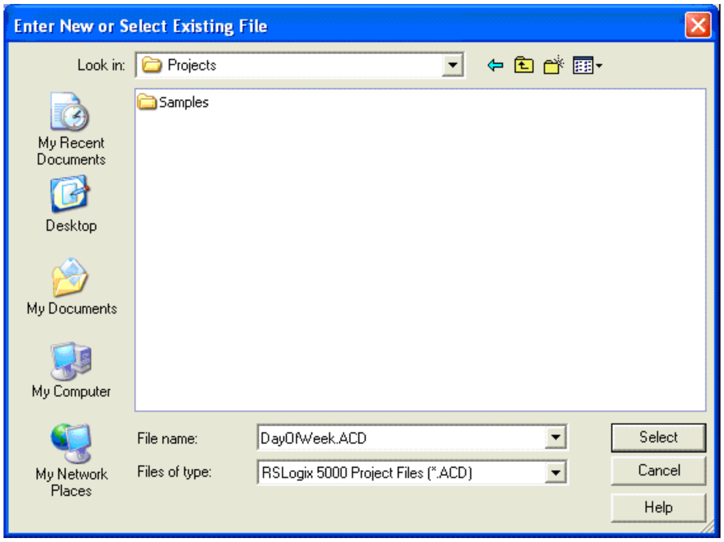


Condition: The project file 'DayOfWeek.ACD' was not found in your project directory.
Select new or existing project file.

Connected Controller:
Controller Name: DayOfWeek
Controller Type: 1756-L63/A ControlLogix5563 Controller
Comm Path: AB_ETH-1\192.168.1.4\Backplane\0
Serial Number: 0014CF89
Security: No Protection

Offline Project:
Controller Name:

3. Click **Select file** to find the project file or to identify a location to save the project file.
4. Identify a file and click **Select**.



Enter New or Select Existing File

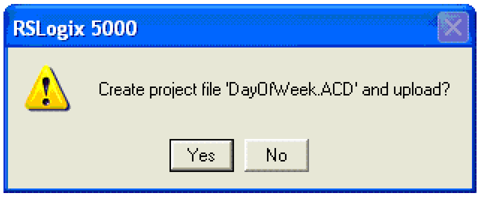
Look in: Projects

Samples

File name: DayOfWeek.ACD

Files of type: RSLogix 5000 Project Files (*.ACD)

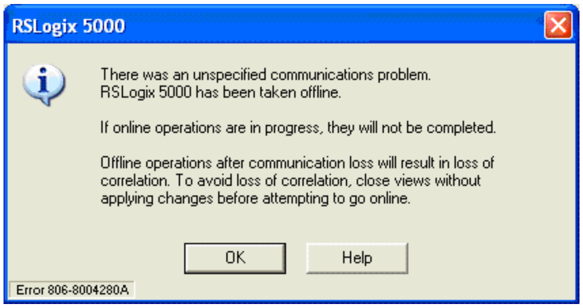
5. Click **Yes**.



RSLogix 5000

Create project file 'DayOfWeek.ACD' and upload?

An unspecified communications dialog box appears.



RSLogix 5000

There was an unspecified communications problem.
RSLogix 5000 has been taken offline.

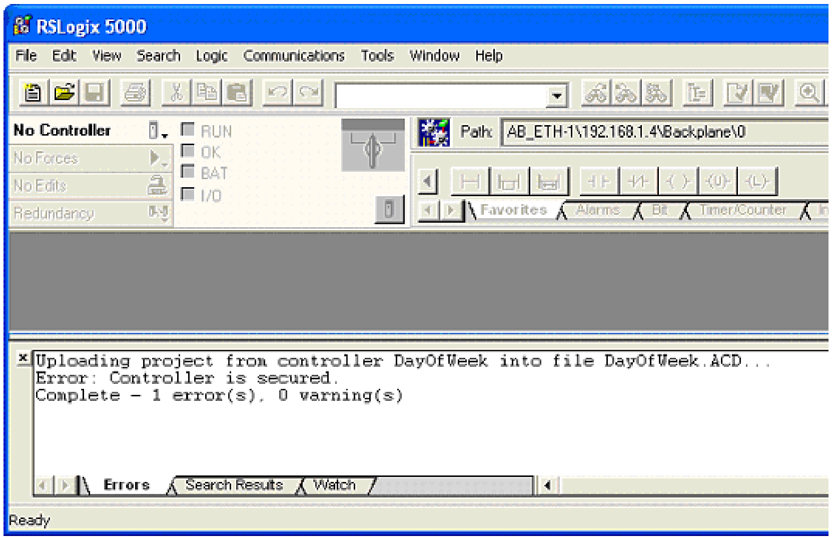
If online operations are in progress, they will not be completed.

Offline operations after communication loss will result in loss of correlation. To avoid loss of correlation, close views without applying changes before attempting to go online.

Error 806-8004280A

6. Click **OK** to continue.

If the project file already exists on your system, an error message is displayed that indicates that the controller is secured and you cannot go online.

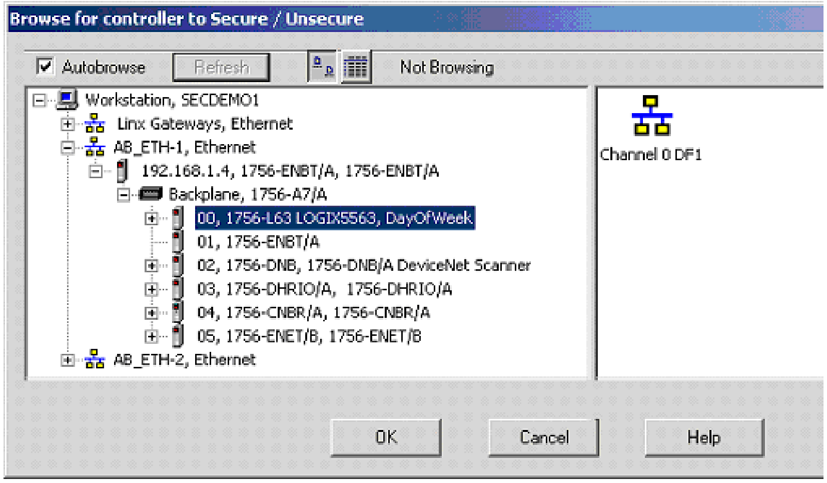


```
Uploading project from controller DayOfWeek into file DayOfWeek.ACD...
Error: Controller is secured.
Complete - 1 error(s), 0 warning(s)
```

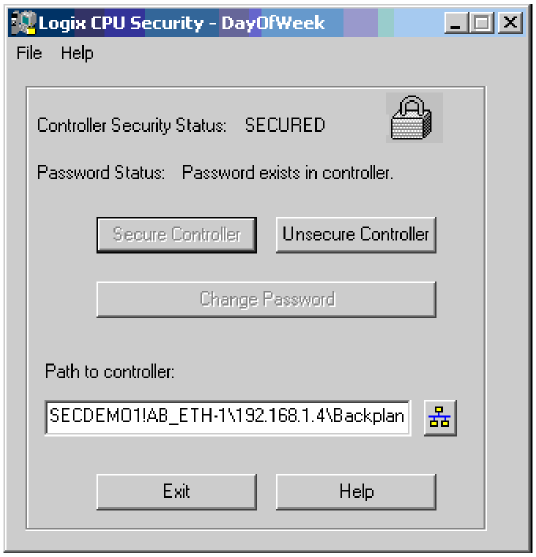
Removing Security from a Controller with the CPU Security Tool

Do these steps to remove security from a controller.

1. Launch the Logix CPU Security Tool.
2. Use RSWho to specify the path to the controller.
3. Select the controller that you want to be unsecured and click **OK**.


Browse for controller to Secure / Unsecure
Autobrowse
Refresh
Not Browsing
Workstation, SECDEMO1
Linx Gateways, Ethernet
AB_ETH-1, Ethernet
192.168.1.4, 1756-ENBT/A, 1756-ENBT/A
Backplane, 1756-A7/A
00, 1756-L63 LOGIX5563, DayOfWeek
01, 1756-ENBT/A
02, 1756-DNB, 1756-DNB/A DeviceNet Scanner
03, 1756-DHRIO/A, 1756-DHRIO/A
04, 1756-CNBR/A, 1756-CNBR/A
05, 1756-ENET/B, 1756-ENET/B
AB_ETH-2, Ethernet
Channel 0 DF1
OK
Cancel
Help

4. Select **Unsecure Controller**.



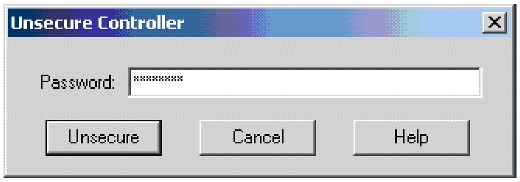
Logix CPU Security - DayOfWeek

Controller Security Status: SECURED

Password Status: Password exists in controller.

Path to controller: SECDEMO1!AB_ETH-1\192.168.1.4\Backplan

5. Enter the password for the controller and click **Unsecure**.



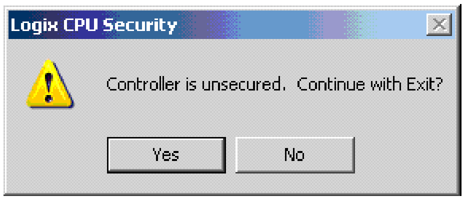
Unsecure Controller

Password: ********

The controller is now unsecured, but the controller still recognizes the password.

6. Select **Exit**.

7. Click **Yes**.



Logix CPU Security

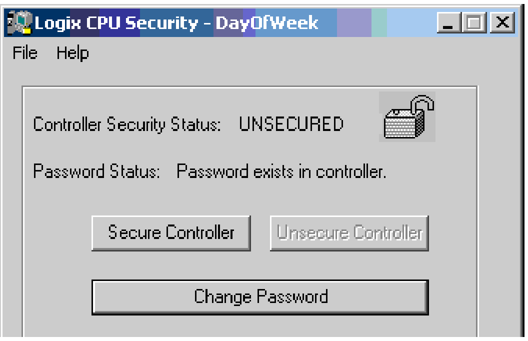
Controller is unsecured. Continue with Exit?

You can now go online with the controller.

Removing a Password

Do these steps to remove a password.

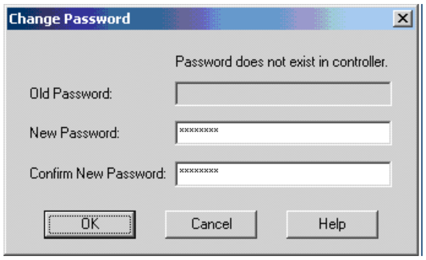
1. Click **Change Password**.



Controller Security Status: UNSECURED

Password Status: Password exists in controller.

2. Remove the '****' empty string and click **OK**.



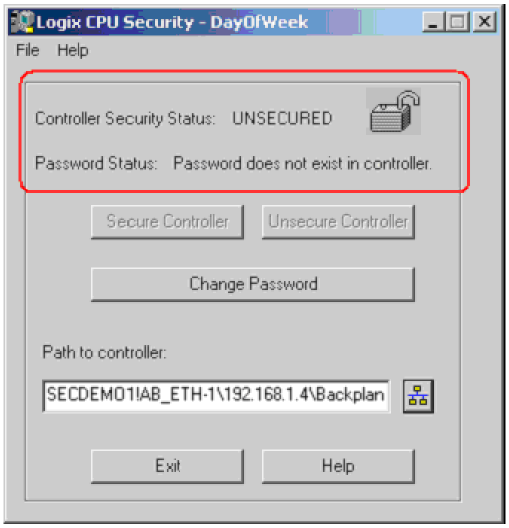
Password does not exist in controller.

Old Password:

New Password: ********

Confirm New Password: ********

The controller status is now UNSECURED.



Controller Security Status: UNSECURED

Password Status: Password does not exist in controller.

Path to controller:

SECDEMO1!AB_ETH-1\192.168.1.4\Backplan

Notes:

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support/, you can find technical manuals, a knowledge base of FAQs, technical and application notes, sample code and links to software service packs, and a MySupport feature that you can customize to make the best use of these tools.

For an additional level of technical phone support for installation, configuration, and troubleshooting, we offer TechConnect support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/support/.

Installation Assistance

If you experience a problem within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/support/americas/phone_en.html, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

Rockwell Otomasyon Ticaret A.Ş., Kar Plaza İş Merkezi E Blok Kat:6 34752 İçerenköy, İstanbul, Tel: +90 (216) 5698400

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Supersedes Publication 1756-PM016D-EN-P - September 2010